



Lori A. Shibanette
Commissioner

Lisa M. Morris
Director

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
DIVISION OF PUBLIC HEALTH SERVICES

29 HAZEN DRIVE, CONCORD, NH 03301
603-271-4501 1-800-852-3345 Ext. 4501
Fax: 603-271-4827 TDD Access: 1-800-735-2964
www.dhhs.nh.gov

September 28, 2020

His Excellency, Governor Christopher T. Sununu
and the Honorable Council
State House
Concord, New Hampshire 03301

REQUESTED ACTION

Authorize the Department of Health and Human Services, Division of Public Health Services, to enter into a **Retroactive Sole Source** amendment to an existing contract with Motorola Solutions, Inc., formerly known as Airbus DS Communications, Inc., (VC# TBD), Temecula, CA for continual maintenance and support of the Communicator NXT system, by exercising a renewal option by increasing the price limitation by \$39,333 from \$198,950 to \$238,283 and by extending the completion date from August 31, 2020 to August 31, 2021 effective upon Governor and Council approval. 100% Federal Funds.

The original contract was approved by Governor and Council on October 7, 2015, item #15.

Funds are available in the following account for State Fiscal Year 2021, and are anticipated to be available in State Fiscal Year 2022, upon the availability and continued appropriation of funds in the future operating budget, with the authority to adjust budget line items within the price limitation and encumbrances between state fiscal years through the Budget Office, if needed and justified.

05-95-90-902510-5084, HEALTH AND SOCIAL SERVICES, DEPT OF HEALTH AND HUMAN SERVICES, HHS: DIVISION OF PUBLIC HEALTH, BUREAU OF INFECTIOUS DISEASE CONTROL, EBOLA GRANT

Fiscal Year	Class/Object	Class Title	Job Number	Current Budget	Increased (Decreased) Amount	Revised Budget
2016	102-500731	Contracts for Prog Svc.	90027030	\$33,208	\$0	\$33,208
2017	102-500731	Contracts for Prog Svc.	90027030	\$6,642	\$0	\$6,642
			Sub-Total	\$39,850	\$0	\$39,850

05-95-90-902510-7545, HEALTH AND SOCIAL SERVICES, DEPT OF HEALTH AND HUMAN SERVICES, HHS: DIVISION OF PUBLIC HEALTH, BUREAU OF INFECTIOUS DISEASE CONTROL, EMERGENCY PREPAREDNESS

Fiscal Year	Class/Object	Class Title	Job Number	Current Budget	Increased (Decreased) Amount	Revised Budget
2017	102-500731	Contracts for Prog Svc.	90077002	\$35,458	\$0	\$35,458
2018	102-500731	Contracts for Prog Svc.	90077002	\$39,467	\$0	\$39,467
2019	102-500731	Contracts for Prog Svc.	90077002	\$38,850	\$0	\$38,850
2020	102-500731	Contracts for Prog Svc.	90077002	\$38,850	\$0	\$38,850
2021	102-500731	Contracts for Prog Svc.	90077002	\$6,475	\$0	\$6,475
			Sub-Total	\$159,100	\$0	\$159,100

05-95-90-902510-7039, HEALTH AND SOCIAL SERVICES, DEPT OF HEALTH AND HUMAN SERVICES, HHS: DIVISION OF PUBLIC HEALTH, BUREAU OF INFECTIOUS DISEASE CONTROL, PUBLIC HEALTH CRISIS RESPONSE

Fiscal Year	Class/Object	Class Title	Job Number	Current Budget	Increased (Decreased) Amount	Revised Budget
2021	102500731	Contracts for Prog Svc.	90027027	\$0	\$34,168	\$34,168
2022	102500731	Contracts for Prog Svc.	90027027	\$0	\$5,165	\$5,165
			Sub-Total	\$0	\$39,333	\$39,333
			Total	\$198,950	\$39,333	\$238,283

EXPLANATION

This request is **Retroactive** because more time was needed to negotiate and finalize the scope of the work prior to the vendor accepting the terms of the agreement. This request is **Sole Source** because the original contract was approved as sole source and MOP 150 requires any subsequent amendments to be labelled as sole source. Additionally, the vendor is uniquely qualified to host and support the Communicator NXT System as they have provided maintenance, support, and back up services to the State for the in-house hosted hardware and software for the Communicator NXT System since 2002. No other vendor is able to host and maintain this proprietary System.

The purpose of this request is for the Department to continue to host the Communicator NXT system, the platform that runs the NH Health Alert Network. The Communicator NXT System is a web-based, high-speed notification system used by the Department and other internal and external partners to communicate with health professionals, agencies and institutions in the event of a public health alert or advisory. The System is used to send out approximately 20 – 30 health alerts each year as well as activate the Public Health Incident Management Team during emergencies.

The vendor will continue to provide continual support and maintenance of the system. The vendor also supports a redundant system so that access is always available in the event the main servers are down for maintenance or during system failures.

The Department will monitor contracted services using the following performance measures:

- Less than 1% in system downtime.
- Complete repair and maintenance as requested by the Department
- Monitor the system performance on an ongoing basis

As referenced in Part 2, Exhibit C Special Provisions of the original contract, the parties have the option to extend the agreement for up to four (4) additional years, contingent upon satisfactory delivery of services, available funding, agreement of the parties and Governor and Council approval. The Department is exercising its option to renew services for one (1) of the four (4) years available.

Should the Governor and Council not authorize this request loss of ability to communicate directly with over 16,000 health care providers and other stakeholders about critical public health issues.

Area served: Statewide

Source of Funds: CFDA #93.354, FAIN # NU90TP922106-01-00

In the event that the Federal Funds become no longer available, General Funds will not be requested to support this program.

Respectfully submitted,



Lori A. Shabinette
Commissioner



STATE OF NEW HAMPSHIRE
DEPARTMENT OF INFORMATION TECHNOLOGY
27 Hazen Dr., Concord, NH 03301
Fax: 603-271-1516 TDD Access: 1-800-735-2964
www.nh.gov/doit

Denis Goulet
Commissioner

September 24, 2020

Lori A. Shibinette, Commissioner
Department of Health and Human Services
State of New Hampshire
129 Pleasant Street
Concord, NH 03301

Dear Commissioner Shibinette:

This letter represents formal notification that the Department of Information Technology (DoIT) has approved your agency's request to enter into a Retroactive Sole Source contract amendment with Motorola Solutions, Inc. f/k/a Airbus DS Communications, Inc. of Temecula, CA as described below and referenced as DoIT No. 2015-049A.

The purpose of this amendment is to provide for hosting, maintenance and support of the NH Health Alert Network. The Division of Public Health Services issues between 20 and 30 Health Alerts annually to inform clinicians statewide about a broad range of public health issues. During emergencies such as COVID-19 the number of Health Alerts increases significantly as the DPHS provides updates guidance and other information to clinicians.

The funding amount for this amendment is \$39,333, increasing the current contract from \$198,950 to \$238,283 and by extending the completion date to August 31, 2021 from the original completion date of August 31, 2020. This amendment shall become effective retroactive to September 1, 2020 through August 31, 2021 upon Governor and Executive Council approval.

A copy of this letter should accompany the Department of Health and Human Services' submission to the Governor and Executive Council for approval.

Sincerely,

Denis Goulet

DG/kaf
DoIT #2015-049A
RID: N/A
cc: Michael Williams, IT Manager, DoIT



**New Hampshire Department of Health and Human Services
Communicator Hosting, Maintenance and Support Services**

**State of New Hampshire
Department of Health and Human Services
Amendment #1 to the Communicator Hosting, Maintenance and Support Services**

This 1st Amendment to the Communicator Hosting, Maintenance and Support Services contract (hereinafter referred to as "Amendment #1") is by and between the State of New Hampshire, Department of Health and Human Services (hereinafter referred to as the "State" or "Department") and Motorola Solutions, Inc., formerly known as Airbus DS Communications, Inc., (hereinafter referred to as "the Contractor"), a corporation with a place of business at 42505 Rio Nedo Temecula, CA, 92590

WHEREAS, pursuant to an agreement (the "Contract") approved by the Governor and Executive Council on October 7, 2015, (Item #15), the Contractor agreed to perform certain services based upon the terms and conditions specified in the Contract and in consideration of certain sums specified; and

WHEREAS, pursuant to Contract Agreement – Part 1, Form P-37, General Provisions, Paragraph 18 and Contract Agreement – Part 3, Exhibit C, Section 1, Subsection 1.18, the Contract may be amended upon written agreement of the parties and approval from the Governor and Executive Council; and

WHEREAS, the parties agree to extend the term of the agreement, increase the price limitation, or modify the scope of services to support continued delivery of these services; and

NOW THEREFORE, in consideration of the foregoing and the mutual covenants and conditions contained in the Contract and set forth herein, the parties hereto agree to amend as follows:

1. Contract Agreement – Part 1, Form P-37 General Provisions, Block 1.3, Contractor Name, to read:
Motorola Solutions, Inc.
2. Contract Agreement – Part 1, Form P-37 General Provisions, Block 1.4, Contractor Address, to read:
42505 Rio Nedo Rd.
Temecula, CA, 92590
3. Contract Agreement – Part 1, Form P-37 General Provisions, Block 1.4, Completion Phone Number, to read:
951-719-2100
4. Contract Agreement – Part 1, Form P-37 General Provisions, Block 1.7, Completion Date, to read:
August 31, 2021.
5. Contract Agreement – Part 1, Form P-37, General Provisions, Block 1.8, Price Limitation, to read:
\$238,283.
6. Contract Agreement – Part 1, Form P-37, General Provisions, Block 1.9, Contracting Officer for State Agency, to read:
Nathan D. White, Director.
7. Contract Agreement – Part 1, Form P-37, General Provisions, Block 1.10, State Agency Telephone Number, to read:
603-271-9631.
8. Modify Contract Agreement - Part 2; Contract Agreement – Part 3; and any attachments by deleting references to "Airbus," "Airbus DS," "Airbus DS Communications," and "Airbus DS Communications, Inc.," and replacing such references with, "Contractor," or "the Contractor," as



New Hampshire Department of Health and Human Services Communicator Hosting, Maintenance and Support Services

appropriate.

9. Modify Contract Agreement – Part 2, Section 3 Contract Management, Subsection 3.1, to read:

3.1 Contractor's Contract Manager

The Contractor shall assign a Contract Manager who shall be responsible for all Contract authorization and administration. The Contractor shall provide the name and contact information of the Contractor's Contract Manager to DHHS within five (5) business days of the contract effective date or date of change in Contract Manager, whichever is later.

10. Modify Contract Agreement – Part 2, Section 3 Contract Management, Subsection 3.2, Paragraph 3.2.5, to read:

3.2.5 The Contract shall assign a Project Manager and shall provide the name and contact information of the Contractor's Project manager to DHHS within five (5) business days of the contract effective date or date of change in the Project Manager, whichever is later.

11. Modify Contract Agreement – Part 2, Section 3 Contract Management, Subsection 3.3, Paragraph 3.3.3., Subparagraph 3.3.3.1 to read:

3.3.3.1 The Contractor shall assign Key Project Staff and shall provide the names and contact information for each staff to DHHS within five (5) business days of the contract effective date or date of change in the Key Project Staff, whichever is later.

12. Modify Contract Agreement – Part 3, Exhibit A, Contract Deliverables, Section 2 Deliverables, Milestones, and Activities Schedule, Table 2.1 Implementation Schedule – Activities / Deliverables / Milestones, by adding Licensing, Hosting Maintenance and Support, Add-On Modules, and Training: Year 6 lines 21-23 to read:

Reference Number	Activity, Deliverable, or Milestone	Deliverable Type	Projected Delivery Date
Licensing, Hosting Maintenance and Support, Add-On Modules, and Training: Year 6			
21	License Fee (Includes Hosting Maintenance and Support for 17,000 contacts): Year 6	Software & Non-Software	8/31/2021
22	<ul style="list-style-type: none"> Conference Bridge @ \$2,500/year: Year 6 Efax @ \$7,350/year: Year 6 NXT Call Blast @ \$2,500/year: Year 6 	Software	
23	Web-Based Training for up to 10 participants (in addition to the one free session per year): Year 6	Non-Software	

13. Modify Exhibit B, Payment Schedule, Section 1 Deliverable Payment Schedule, Subsection 1.1 Not to Exceed Price to read:

1.1 Not to Exceed Price

This is a Not to Exceed Price (NTE) Contract for Software as a Service (SaaS) totaling the contract Price Limitation in Contract Agreement – Part 1, Form P-37, Block 1.8 for the period between the Effective Date of Governor and Executive Council approval through the Contract Completion Date.



New Hampshire Department of Health and Human Services Communicator Hosting, Maintenance and Support Services

The Contractor shall be responsible for performing its obligations in accordance with the Contract. This Contractor shall invoice the State for the activities in Table 1.1.1 – Deliverable Payment Schedule.

14. Modify Contract Agreement – Part 3, Exhibit B, Payment Schedule, Section 1 Deliverable Payment Schedule, Table 1.1.1 Deliverable Payment Schedule, by adding Licensing, Hosting Maintenance and Support, Add-On Modules, and Training Year 6 lines 21-24 to read:

Deliverable Payment Schedule					
Reference Number	Activity, Deliverable, or Milestone	Deliverable Type	Projected Delivery Date	Price	Payment Amount
Licensing, Hosting Maintenance and Support, Add-On Modules, and Training: Year 6					
21	License Fee (Includes Hosting Maintenance and Support for 17,000 contacts): Year 6	Software & Non-Software	08/31/2021	\$19,500	\$19,500
22	<ul style="list-style-type: none"> Conference Bridge @ \$1,874/year: Year 6 Efax @ \$15,585/year: Year 6 NXT Call Blast @ \$1,874/year: Year 6 	Software		\$19,333	\$19,333
23	Web-Based Training for up to 10 participants (in addition to the one free session per year): Year 6	Non-Software		\$500	\$500
24	Subtotal Ongoing Hosting Maintenance and Support, Add-On Modules, Training: Year 6			\$39,333	\$39,333
	Not to Exceed Total			\$238,283	\$238,283

15. Modify Contract Agreement – Part 3, Exhibit B, Payment Schedule, Section 1 Deliverable Payment Schedule, Table 1.1.2 Detailed License Deliverables and Pricing, by adding Table 1.1.2a – Detailed License Deliverables and Pricing for Year 6 to read:

Table 1.1.2 – Detailed License Deliverables and Pricing for Year 6

Detailed License Deliverables and Pricing			
Description	License Type	Quantity	Net Price-License
SaaS			
License (Includes Hosting Maintenance and Support for 17,000 contacts)	non-exclusive, non-transferable, worldwide term	1	\$19,500
Application Products			
XML API		1	Included
In-Bound Bulletin Board		1	Included



New Hampshire Department of Health and Human Services Communicator Hosting, Maintenance and Support Services

EFax		1	\$15,585
NXT Call Blast		1	\$1,874
Conference Bridge		1	\$1,874
Web-based training		1	\$500
Grand Total			\$39,333

16. Modify Contract Agreement – Part 3, Exhibit B, Payment Schedule, Section 1 Deliverable Payment Schedule, Table 1.1.3 Airbus SaaS, to read:

Contractor SaaS Pricing Worksheet						
SaaS	9/1/2015-8/31/2016	9/1/2016-8/31/2017	9/1/2017-8/31/2018	9/1/2018-8/31/2019	9/1/2019-8/31/2020	9/1/2020-8/31/2021
License (Includes Hosting Maintenance and Support for 9,000 contacts)	\$26,000	\$26,000	\$26,000	\$26,000	\$26,000	\$19,500
Implementation Processes (one-time charge)	\$1,500	\$0.00	\$0.00	\$0.00	\$0.00	0
Onsite training for 5 participants	\$0.00	\$4,200	\$0.00	\$0.00	\$0.00	0
Additional Annual Web-Training	\$0.00	\$0.00	\$500	\$500	\$500	\$500
Application Products						
XML API	Included	Included	Included	Included	Included	Included
In-Bound Bulletin Board	Included	Included	Included	Included	Included	Included
EFax	\$7,350	\$7,350	\$7,350	\$7,350	\$7,350	\$15,585
NXT Call Blast	\$2,500	\$2,500	\$2,500	\$2,500	\$2,500	\$1,874
Conference Bridge	\$2,500	\$2,500	\$2,500	\$2,500	\$2,500	\$1,874

17. Modify Contract Agreement – Part 3, Exhibit B, Payment Schedule, Section 2 Total Contract Price to read:

2. Total Contract Price

Notwithstanding any provision in the Contract to the contrary, and notwithstanding unexpected circumstances, in no event shall the total of all payments made by the State exceed the Contract Price Limitation in Block 1.8, Contract Agreement – Part 1, Form P37, General Provisions.

The State will not be responsible for any travel or out of pocket expenses incurred in the



**New Hampshire Department of Health and Human Services
Communicator Hosting, Maintenance and Support Services**

performance of the Services performed under this Contract.

18. Modify Contract Agreement – Part 3, Exhibit B, Section 4, Payment Address to read:

4. Payment Address

All payments shall be sent to the following address:

Motorola Solutions, Inc.
42505 Rio Nedo
Temecula, CA, 92590

19. Modify Contract Agreement – Part 3, Exhibit O, Special Exhibits, Attachments, and Certificates, Section 1 Attachment 1 – Department of health and Human Services Exhibits D through J, to read:

1. Attachment 1 – Department of Health and Human Services Exhibits D through J and Exhibit K.

20. Modify Contract Agreement – Part 3, Exhibit O, Special Exhibits, Attachments and Certificates, Section 1, by adding Exhibit K, DHHS Information Security Requirements, which is attached hereto and incorporated by reference herein.



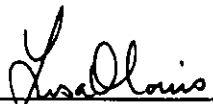
**New Hampshire Department of Health and Human Services
Communicator Hosting, Maintenance and Support Services**

All terms and conditions of the Contract not inconsistent with this Amendment #1 remain in full force and effect. This amendment shall be effective upon the date of Governor and Executive Council approval.

IN WITNESS WHEREOF, the parties have set their hands as of the date written below,

State of New Hampshire
Department of Health and Human Services

10/1/2020
Date


Name: Lisa Morris
Title: Director, Division of Public Health Services

Motorola Solutions, Inc.

10/1/2020
Date

DocuSigned by:

Name: Michael Anderson
Title: sales Director - North America



**New Hampshire Department of Health and Human Services
Communicator Hosting, Maintenance and Support Services**

The preceding Amendment, having been reviewed by this office, is approved as to form, substance, and execution.

OFFICE OF THE ATTORNEY GENERAL

10/12/20

Date

Catherine Pinos

Name: Catherine Pinos, Attorney
Title:

I hereby certify that the foregoing Amendment was approved by the Governor and Executive Council of the State of New Hampshire at the Meeting on: _____ (date of meeting)

OFFICE OF THE SECRETARY OF STATE

Date

Name:
Title:

New Hampshire Department of Health and Human Services**Exhibit K****DHHS Information Security Requirements****A. Definitions**

The following terms may be reflected and have the described meaning in this document:

1. "Breach" means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic. With regard to Protected Health Information, "Breach" shall have the same meaning as the term "Breach" in section 164.402 of Title 45, Code of Federal Regulations.
2. "Computer Security Incident" shall have the same meaning "Computer Security Incident" in section two (2) of NIST Publication 800-61, Computer Security Incident Handling Guide, National Institute of Standards and Technology, U.S. Department of Commerce.
3. "Confidential Information" or "Confidential Data" means all confidential information disclosed by one party to the other such as all medical, health, financial, public assistance benefits and personal information including without limitation, Substance Abuse Treatment Records, Case Records, Protected Health Information and Personally Identifiable Information.

Confidential Information also includes any and all information owned or managed by the State of NH - created, received from or on behalf of the Department of Health and Human Services (DHHS) or accessed in the course of performing contracted services - of which collection, disclosure, protection, and disposition is governed by state or federal law or regulation. This information includes, but is not limited to Protected Health Information (PHI), Personal Information (PI), Personal Financial Information (PFI), Federal Tax Information (FTI), Social Security Numbers (SSN), Payment Card Industry (PCI), and or other sensitive and confidential information.

4. "End User" means any person or entity (e.g., contractor, contractor's employee, business associate, subcontractor, other downstream user, etc.) that receives DHHS data or derivative data in accordance with the terms of this Contract.
5. "HIPAA" means the Health Insurance Portability and Accountability Act of 1996 and the regulations promulgated thereunder.
6. "Incident" means an act that potentially violates an explicit or implied security policy, which includes attempts (either failed or successful) to gain unauthorized access to a system or its data, unwanted disruption or denial of service, the unauthorized use of a system for the processing or storage of data; and changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent. Incidents include the loss of data through theft or device misplacement, loss or misplacement of hardcopy documents, and misrouting of physical or electronic

DS
[Signature]

New Hampshire Department of Health and Human Services

Exhibit K

DHHS Information Security Requirements



mail, all of which may have the potential to put the data at risk of unauthorized access, use, disclosure, modification or destruction.

7. "Open Wireless Network" means any network or segment of a network that is not designated by the State of New Hampshire's Department of Information Technology or delegate as a protected network (designed, tested, and approved, by means of the State, to transmit) will be considered an open network and not adequately secure for the transmission of unencrypted PI, PFI, PHI or confidential DHHS data.
8. "Personal Information" (or "PI") means information which can be used to distinguish or trace an individual's identity, such as their name, social security number, personal information as defined in New Hampshire RSA 359-C:19, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.
9. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Parts 160 and 164, promulgated under HIPAA by the United States Department of Health and Human Services.
10. "Protected Health Information" (or "PHI") has the same meaning as provided in the definition of "Protected Health Information" in the HIPAA Privacy Rule at 45 C.F.R. § 160.103.
11. "Security Rule" shall mean the Security Standards for the Protection of Electronic Protected Health Information at 45 C.F.R. Part 164, Subpart C, and amendments thereto.
12. "Unsecured Protected Health Information" means Protected Health Information that is not secured by a technology standard that renders Protected Health Information unusable, unreadable, or indecipherable to unauthorized individuals and is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute.

I. RESPONSIBILITIES OF DHHS AND THE CONTRACTOR

A. Business Use and Disclosure of Confidential Information.

1. The Contractor must not use, disclose, maintain or transmit Confidential Information except as reasonably necessary as outlined under this Contract. Further, Contractor, including but not limited to all its directors, officers, employees and agents, must not use, disclose, maintain or transmit PHI in any manner that would constitute a violation of the Privacy and Security Rule.
2. The Contractor must not disclose any Confidential Information in response to a

New Hampshire Department of Health and Human Services

Exhibit K

DHHS Information Security Requirements



request for disclosure on the basis that it is required by law, in response to a subpoena, etc., without first notifying DHHS so that DHHS has an opportunity to consent or object to the disclosure.

3. If DHHS notifies the Contractor that DHHS has agreed to be bound by additional restrictions over and above those uses or disclosures or security safeguards of PHI pursuant to the Privacy and Security Rule, the Contractor must be bound by such additional restrictions and must not disclose PHI in violation of such additional restrictions and must abide by any additional security safeguards.
4. The Contractor agrees that DHHS Data or derivative there from disclosed to an End User must only be used pursuant to the terms of this Contract.
5. The Contractor agrees DHHS Data obtained under this Contract may not be used for any other purposes that are not indicated in this Contract.
6. The Contractor agrees to grant access to the data to the authorized representatives of DHHS for the purpose of inspecting to confirm compliance with the terms of this Contract.

II. METHODS OF SECURE TRANSMISSION OF DATA

1. Application Encryption. If End User is transmitting DHHS data containing Confidential Data between applications, the Contractor attests the applications have been evaluated by an expert knowledgeable in cyber security and that said application's encryption capabilities ensure secure transmission via the internet.
2. Computer Disks and Portable Storage Devices. End User may not use computer disks or portable storage devices, such as a thumb drive, as a method of transmitting DHHS data.
3. Encrypted Email. End User may only employ email to transmit Confidential Data if email is encrypted and being sent to and being received by email addresses of persons authorized to receive such information.
4. Encrypted Web Site. If End User is employing the Web to transmit Confidential Data, the secure socket layers (SSL) must be used and the web site must be secure. SSL encrypts data transmitted via a Web site.
5. File Hosting Services, also known as File Sharing Sites. End User may not use file hosting services, such as Dropbox or Google Cloud Storage, to transmit Confidential Data.
6. Ground Mail Service. End User may only transmit Confidential Data via *certified* ground mail within the continental U.S. and when sent to a named individual.
7. Laptops and PDA. If End User is employing portable devices to transmit Confidential Data said devices must be encrypted and password-protected.
8. Open Wireless Networks. End User may not transmit Confidential Data via an open

DS
JA

New Hampshire Department of Health and Human Services**Exhibit K****DHHS Information Security Requirements**

wireless network. End User must employ a virtual private network (VPN) when remotely transmitting via an open wireless network.

9. Remote User Communication. If End User is employing remote communication to access or transmit Confidential Data, a virtual private network (VPN) must be installed on the End User's mobile device(s) or laptop from which information will be transmitted or accessed.
10. SSH File Transfer Protocol (SFTP), also known as Secure File Transfer Protocol. If End User is employing an SFTP to transmit Confidential Data, End User will structure the Folder and access privileges to prevent inappropriate disclosure of information. SFTP folders and sub-folders used for transmitting Confidential Data will be coded for 24-hour auto-deletion cycle (i.e. Confidential Data will be deleted every 24 hours).
11. Wireless Devices. If End User is transmitting Confidential Data via wireless devices, all data must be encrypted to prevent inappropriate disclosure of information.

III. RETENTION AND DISPOSITION OF IDENTIFIABLE RECORDS

The Contractor will only retain the data and any derivative of the data for the duration of this Contract. After such time, the Contractor will have 30 days to destroy the data and any derivative in whatever form it may exist, unless, otherwise required by law or permitted under this Contract. To this end, the parties must:

A. Retention

1. The Contractor agrees it will not store, transfer or process data collected in connection with the services rendered under this Contract outside of the United States. This physical location requirement shall also apply in the implementation of cloud computing, cloud service or cloud storage capabilities, and includes backup data and Disaster Recovery locations.
2. The Contractor agrees to ensure proper security monitoring capabilities are in place to detect potential security events that can impact State of NH systems and/or Department confidential information for contractor provided systems.
3. The Contractor agrees to provide security awareness and education for its End Users in support of protecting Department confidential information.
4. The Contractor agrees to retain all electronic and hard copies of Confidential Data in a secure location and identified in section IV. A.2
5. The Contractor agrees Confidential Data stored in a Cloud must be in a FedRAMP/HITECH compliant solution and comply with all applicable statutes and regulations regarding the privacy and security. All servers and devices must have currently-supported and hardened operating systems, the latest anti-viral, anti-hacker, anti-spam, anti-spyware, and anti-malware utilities. The environment, as a

DS

New Hampshire Department of Health and Human Services**Exhibit K****DHHS Information Security Requirements**

whole, must have aggressive intrusion-detection and firewall protection.

6. The Contractor agrees to and ensures its complete cooperation with the State's Chief Information Officer in the detection of any security vulnerability of the hosting infrastructure.

B. Disposition

1. If the Contractor will maintain any Confidential Information on its systems (or its sub-contractor systems), the Contractor will maintain a documented process for securely disposing of such data upon request or contract termination; and will obtain written certification for any State of New Hampshire data destroyed by the Contractor or any subcontractors as a part of ongoing, emergency, and or disaster recovery operations. When no longer in use, electronic media containing State of New Hampshire data shall be rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion and media sanitization, or otherwise physically destroying the media (for example, degaussing) as described in NIST Special Publication 800-88, Rev 1, Guidelines for Media Sanitization, National Institute of Standards and Technology, U. S. Department of Commerce. The Contractor will document and certify in writing at time of the data destruction, and will provide written certification to the Department upon request. The written certification will include all details necessary to demonstrate data has been properly destroyed and validated. Where applicable, regulatory and professional standards for retention requirements will be jointly evaluated by the State and Contractor prior to destruction.
2. Unless otherwise specified, within thirty (30) days of the termination of this Contract, Contractor agrees to destroy all hard copies of Confidential Data using a secure method such as shredding.
3. Unless otherwise specified, within thirty (30) days of the termination of this Contract, Contractor agrees to completely destroy all electronic Confidential Data by means of data erasure, also known as secure data wiping.

IV. PROCEDURES FOR SECURITY

- A. Contractor agrees to safeguard the DHHS Data received under this Contract, and any derivative data or files, as follows:
 1. The Contractor will maintain proper security controls to protect Department confidential information collected, processed, managed, and/or stored in the delivery of contracted services.
 2. The Contractor will maintain policies and procedures to protect Department confidential information throughout the information lifecycle, where applicable, (from creation, transformation, use, storage and secure destruction) regardless of the media used to store the data (i.e., tape, disk, paper, etc.).

New Hampshire Department of Health and Human Services**Exhibit K****DHHS Information Security Requirements**

3. The Contractor will maintain appropriate authentication and access controls to contractor systems that collect, transmit, or store Department confidential information where applicable.
4. The Contractor will ensure proper security monitoring capabilities are in place to detect potential security events that can impact State of NH systems and/or Department confidential information for contractor provided systems.
5. The Contractor will provide regular security awareness and education for its End Users in support of protecting Department confidential information.
6. If the Contractor will be sub-contracting any core functions of the engagement supporting the services for State of New Hampshire, the Contractor will maintain a program of an internal process or processes that defines specific security expectations, and monitoring compliance to security requirements that at a minimum match those for the Contractor, including breach notification requirements.
7. The Contractor will work with the Department to sign and comply with all applicable State of New Hampshire and Department system access and authorization policies and procedures, systems access forms, and computer use agreements as part of obtaining and maintaining access to any Department system(s). Agreements will be completed and signed by the Contractor and any applicable sub-contractors prior to system access being authorized.
8. If the Department determines the Contractor is a Business Associate pursuant to 45 CFR 160.103, the Contractor will execute a HIPAA Business Associate Agreement (BAA) with the Department and is responsible for maintaining compliance with the agreement.
9. The Contractor will work with the Department at its request to complete a System Management Survey. The purpose of the survey is to enable the Department and Contractor to monitor for any changes in risks, threats, and vulnerabilities that may occur over the life of the Contractor engagement. The survey will be completed annually, or an alternate time frame at the Departments discretion with agreement by the Contractor, or the Department may request the survey be completed when the scope of the engagement between the Department and the Contractor changes.
10. The Contractor will not store, knowingly or unknowingly, any State of New Hampshire or Department data offshore or outside the boundaries of the United States unless prior express written consent is obtained from the Information Security Office leadership member within the Department.
11. Data Security Breach Liability. In the event of any security breach Contractor shall make efforts to investigate the causes of the breach, promptly take measures to prevent future breach and minimize any damage or loss resulting from the breach. The State shall recover from the Contractor all costs of response and recovery from

New Hampshire Department of Health and Human Services

Exhibit K

DHHS Information Security Requirements



the breach, including but not limited to: credit monitoring services, mailing costs and costs associated with website and telephone call center services necessary due to the breach.

12. Contractor must, comply with all applicable statutes and regulations regarding the privacy and security of Confidential Information, and must in all other respects maintain the privacy and security of PI and PHI at a level and scope that is not less than the level and scope of requirements applicable to federal agencies, including, but not limited to, provisions of the Privacy Act of 1974 (5 U.S.C. § 552a), DHHS Privacy Act Regulations (45 C.F.R. §5b), HIPAA Privacy and Security Rules (45 C.F.R. Parts 160 and 164) that govern protections for individually identifiable health information and as applicable under State law.
13. Contractor agrees to establish and maintain appropriate administrative, technical, and physical safeguards to protect the confidentiality of the Confidential Data and to prevent unauthorized use or access to it. The safeguards must provide a level and scope of security that is not less than the level and scope of security requirements established by the State of New Hampshire, Department of Information Technology. Refer to Vendor Resources/Procurement at <https://www.nh.gov/doit/vendor/index.htm> for the Department of Information Technology policies, guidelines, standards, and procurement information relating to vendors.
14. Contractor agrees to maintain a documented breach notification and incident response process. The Contractor will notify the State's Privacy Officer and the State's Security Officer of any security breach immediately, at the email addresses provided in Section VI. This includes a confidential information breach, computer security incident, or suspected breach which affects or includes any State of New Hampshire systems that connect to the State of New Hampshire network.
15. Contractor must restrict access to the Confidential Data obtained under this Contract to only those authorized End Users who need such DHHS Data to perform their official duties in connection with purposes identified in this Contract.
16. The Contractor must ensure that all End Users:
 - a. comply with such safeguards as referenced in Section IV A. above, implemented to protect Confidential Information that is furnished by DHHS under this Contract from loss, theft or inadvertent disclosure.
 - b. safeguard this information at all times.
 - c. ensure that laptops and other electronic devices/media containing PHI, PI, or PFI are encrypted and password-protected.
 - d. send emails containing Confidential Information only if encrypted and being sent to and being received by email addresses of persons authorized to receive such information.

New Hampshire Department of Health and Human Services**Exhibit K****DHHS Information Security Requirements**

- e. limit disclosure of the Confidential Information to the extent permitted by law.
- f. Confidential Information received under this Contract and individually identifiable data derived from DHHS Data, must be stored in an area that is physically and technologically secure from access by unauthorized persons during duty hours as well as non-duty hours (e.g., door locks, card keys, biometric identifiers, etc.).
- g. only authorized End Users may transmit the Confidential Data, including any derivative files containing personally identifiable information, and in all cases, such data must be encrypted at all times when in transit, at rest, or when stored on portable media as required in section IV above.
- h. in all other instances Confidential Data must be maintained, used and disclosed using appropriate safeguards, as determined by a risk-based assessment of the circumstances involved.
- i. understand that their user credentials (user name and password) must not be shared with anyone. End Users will keep their credential information secure. This applies to credentials used to access the site directly or indirectly through a third party application.

Contractor is responsible for oversight and compliance of their End Users. DHHS reserves the right to conduct onsite inspections to monitor compliance with this Contract, including the privacy and security requirements provided in herein, HIPAA, and other applicable laws and Federal regulations until such time the Confidential Data is disposed of in accordance with this Contract.

V. LOSS REPORTING

The Contractor must notify the State's Privacy Officer and Security Officer of any Security Incidents and Breaches immediately, at the email addresses provided in Section VI.

The Contractor must further handle and report Incidents and Breaches involving PHI in accordance with the agency's documented Incident Handling and Breach Notification procedures and in accordance with 42 C.F.R. §§ 431.300 - 306. In addition to, and notwithstanding, Contractor's compliance with all applicable obligations and procedures, Contractor's procedures must also address how the Contractor will:

1. Identify Incidents;
2. Determine if personally identifiable information is involved in Incidents;
3. Report suspected or confirmed Incidents as required in this Exhibit or P-37;
4. Identify and convene a core response group to determine the risk level of Incidents and determine risk-based responses to Incidents; and

New Hampshire Department of Health and Human Services

Exhibit K

DHHS Information Security Requirements



5. Determine whether Breach notification is required, and, if so, identify appropriate Breach notification methods, timing, source, and contents from among different options, and bear costs associated with the Breach notice as well as any mitigation measures.

Incidents and/or Breaches that implicate PI must be addressed and reported, as applicable, in accordance with NH RSA 359-C:20.

VI. PERSONS TO CONTACT

A. DHHS Privacy Officer:

DHHSPrivacyOfficer@dhhs.nh.gov

B. DHHS Security Officer:

DHHSInformationSecurityOffice@dhhs.nh.gov

Business Information

Business Details

Business Name: MOTOROLA SOLUTIONS, INC.	Business ID: 2591
Business Type: Foreign Profit Corporation	Business Status: Good Standing
Business Creation Date: 05/17/1973	Name in State of Incorporation: MOTOROLA SOLUTIONS, INC.
Date of Formation in Jurisdiction: 05/17/1973	
Principal Office Address: 500 West Monroe Street, Chicago, IL, 60661, USA	Mailing Address: 500 West Monroe Street, Chicago, IL, 60661, USA
Citizenship / State of Incorporation: Foreign/Delaware	
	Last Annual Report Year: 2020
	Next Report Year: 2021
Duration: Perpetual	
Business Email: CLS-CTARMSevidence@wolterskluwer.com	Phone #: NONE
Notification Email: CLS-CTARMSevidence@wolterskluwer.com	Fiscal Year End Date: NONE

Principal Purpose

S.No	NAICS Code	NAICS Subcode
1	OTHER / TO ENGAGE IN ANY LAWFUL ACT OR ACTIVITY FOR WHICH CORPORATIONS MAY BE ORGANIZED	

Principals Information

Name/Title	Business Address
Gregory Q Brown / Director	500 West Monroe Street, Chicago, IL, 60661, USA
Kenneth D Denman / Director	500 West Monroe Street, Chicago, IL, 60661, USA
Egon P Durban / Director	500 West Monroe Street, Chicago, IL, 60661, USA
Clayton M Jones / Director	500 West Monroe Street, Chicago, IL, 60661, USA
Judy Lewent / Director	500 West Monroe Street, Chicago, IL, 60661, USA

1 Page 1 of 4, records 1 to 5 of 17

Registered Agent Information

Name: C T Corporation System

Registered Office 2 1/2 Beacon Street, Concord, NH, 03301 - 4447, USA
Address:

Registered Mailing 2 1/2 Beacon Street, Concord, NH, 03301 - 4447, USA
Address:

Trade Name Information

Business Name	Business ID	Business Status
AVONT INNOVATIONS (/online/BusinessInquire/TradeNameInformation? 274155 businessID=326955)		Expired

Trade Name Owned By

Name	Title	Address
------	-------	---------

Trademark Information

Trademark Number	Trademark Name	Business Address	Mailing Address
No records to view.			

[Filing History](#) [Address History](#) [View All Other Addresses](#) [Name History](#)
[Shares](#) [Businesses Linked to Registered Agent](#) [Return to Search](#) [Back](#)

NH Department of State, 107 North Main St, Room 204, Concord, NH 03301 -- **[Contact Us \(/online/Home/ContactUS\)](#)**

Version 2.1 © 2014 PCC Technology Group, LLC, All Rights Reserved.

CERTIFICATE OF ASSISTANT SECRETARY
MOTOROLA SOLUTIONS, INC.

The undersigned certifies that he or she is a duly appointed Assistant Secretary of Motorola Solutions, Inc. (the "Company"), a corporation duly organized and existing under the laws of the State of Delaware, and that, as such, he or she is authorized to execute this Certificate on behalf of the Company, and further certifies that:

1. At a meeting of the Board of Directors of the Company held on May 11, 2020 at which a quorum was present and acting throughout, the following resolutions were duly adopted, effective May 11, 2020, have not been amended, and are in full force and effect on the date hereof:

RESOLVED, that all Senior Vice Presidents be, and each one of them is, authorized to sign and execute all agreements, contracts, bids, proposals, deeds, assignments, powers of attorney, performance guarantees, performance guarantee undertakings, instruments, documents, claims, including claims against the United States, and certifications of such claims, in the ordinary course of business of the Company and related to his or her work as a Senior Vice President of one of the Company's businesses, groups or corporate departments, all of which are collectively referred to as "Documents", provided that this authority does not extend to:

a. Documents having a value in excess of \$50 million in the aggregate over the term of the arrangement; or

b. Documents related to: (i) acquisitions, divestitures, joint ventures and equity investments, (ii) outsourcing arrangements, (iii) customer financing extending more than 364 days, (iv) capital expenditures, (v) lease commitments, (vi) agreements and compensatory arrangements applicable to Motorola Solutions Appointed Vice Presidents and above, (vii) litigation and legal claims, (viii) appointing agents and attorneys-in-fact to represent the Company before any customs agency, (ix) financial guarantees, financial surety agreements and financial guarantee undertakings, (x) opening bank accounts, (xi) establishing borrowing relationships on behalf of the Company, and (xii) voting or otherwise dealing with securities owned by the Company. Authority for such Documents is found in the specific resolutions below.

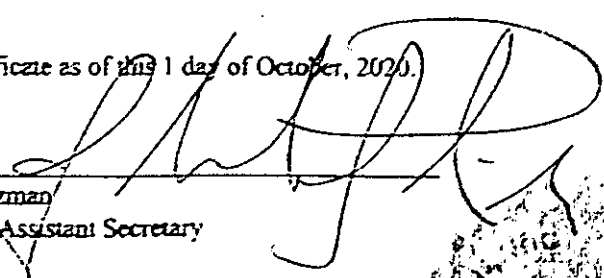
RESOLVED, that the Board has adopted specific resolutions authorizing the signing and execution by Senior Vice Presidents of Documents related to procurement arrangements. Authority for such Documents is found in the specific resolutions below.

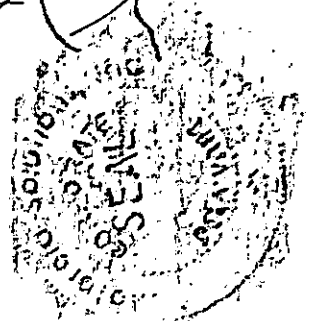
The officers named above are authorized to delegate this signature authority in writing to others.

2. The following person is a duly qualified and acting officer of the Company and has been duly elected to the office set forth opposite his or her name:

Name	Title
Andrew Sinclair	Senior Vice President, General Manager, Software Enterprise Sales

IN WITNESS WHEREOF, I have executed this Certificate as of this 1 day of October, 2020.


John Guzman
Assistant Secretary



SOP E-75 DELEGATION OF AUTHORITY

I, **Andrew Sinclair**, Senior Vice President, General Manager of **Motorola Solutions, Inc.** ("Company"), Software Enterprise Sales, do hereby delegate my authority to approve and execute in the name of and on behalf of the Company, **Vesta Solutions Inc.**, and **Vesta Solutions Communications Corp.**, contract documents (pursuant to Company policy), to the below named individuals with the following dollar and other limitations as specified and explicitly set out below.

Delegation to approve and execute the following Contract documents:

Customer purchase and sale contracts, contract modifications, bids, proposals, bidder list applications, certifications, software licenses, non-disclosure agreements relating to customer sales opportunities, teaming agreements related to customer sales opportunities, lobbyist agreements, and subcontractor documents and other documents which are related Software Sales to the Company.

Region:	To:	Value:
North America	Mike Anderson	\$500,000

This Delegation of Authority granted herein shall not be delegable or assignable to any other person and shall be effective as of **March 18th, 2020** and shall expire on **March 17th, 2021**.

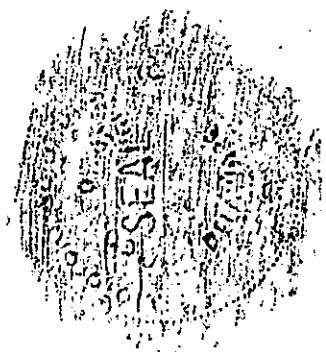
The authority delegated to the above-named individuals is in addition to the authority such individuals may have to approve and execute contract documents as an officer of the Company.

This Delegation can be revoked by me at any time and will automatically expire for any named individual if he or she ceases to be an employee of the Company or if he or she is assigned a different position within the Company. If a named individual is assigned a different position within the Company, the named successor is automatically given the designated authority unless a letter is provided stating otherwise.

IN WITNESS WHEREOF, I have executed this delegation of authority as of **May 20th, 2020**.

Andrew Sinclair
Andrew Sinclair (L-1) (R-1) (R-2)

Andrew Sinclair
Senior Vice President, General Manager, Software Enterprise Sales
Motorola Solutions, Inc.
Senior Vice President
Vesta Solutions, Inc.
Vesta Solutions Communications Corp





MOTOROLA SOLUTIONS

Motorola Solutions, Inc.
500 W. Monroe, Floors 37-44
Chicago, Illinois 60661

Effective: July 29th, 2020

Executive Committee

Gregory Q. Brown	Chairman and Chief Executive Officer
Jason Winkler	Executive Vice President and Chief Financial Officer
Mark S. Hacker	Executive Vice President, General Counsel & Chief Administrative Officer
Kelly Mark	Executive Vice President, Services & Software
Jack Molloy	Executive Vice President, Products & Sales
Rajan Naik	Senior Vice President, Strategy & Ventures
Cynthia Yazdi	Senior Vice President, Chief of Staff, Marketing & Communications
Kristin Kruska	Corporate Vice President and Corporate Secretary

Board of Directors

Gregory Q. Brown
Kenneth D. Denman
Egon P. Durban
Clayton M. Jones
Judy C. Lewent
Gregory K. Mondre
Joseph M. Tucci





9/11/2020

Vesta Solutions, Inc. (Vesta) was acquired by Motorola Solutions, Inc. (Motorola Solutions) in March 2018. In August, Motorola Solutions completed a reorganization of legal entities which is designed to streamline how you do business with Motorola Solutions. As part of that reorganization, Motorola Solutions will now be the legal counterparty to your agreement as it pertains to call-taking and mass notification products and services. Motorola Solutions will assume all of the rights and obligations under your current agreement and continue to provide the same call-taking and mass notification products and services you receive from Vesta. To the extent you have purchased any next-gen core services (NGCS) from Vesta, Vesta will continue to be the provider and legal counterparty for your NGCS contract.

What you need to know

- The delivery of this letter to you represents notice of the assignment of your agreement effective July 13, 2020.
- Assignment of the agreement to Motorola Solutions, Inc. will not alter the performance of services and all terms and conditions of the agreement will remain in full force and effect.
- In conjunction with the reorganization, Vesta's operations were moved to a new ERP. You will notice differences in the invoicing. Every attempt has been made to ensure that all necessary information appears on the invoices. Please notify us if there is pertinent information missing.
- If you have any additional questions, please contact your Customer Success Representative.

What we are requesting from you

- **System Updates:** Please update your systems as necessary in preparation for the restructuring to include Motorola Solutions as a new supplier. Information you may need in order to update your systems is provided on Schedule A to this letter.

We appreciate and thank you for your cooperation and look forward to a continued relationship with the company.

Best regards,

A handwritten signature in black ink, appearing to read 'Geoff Smith', written over a horizontal line.

Geoff Smith
Director of Accounting
Emergency Call Handling Solutions
Motorola Solutions, Inc.



Schedule A: Information to be used for systems set-up

Motorola Solutions, Inc.

Physical Address: Motorola Solutions, Inc.
500 West Monroe
STE 4400
Chicago, IL 60661

FEIN: 36-1115800

Remittance information: Bank information:
Motorola Solutions, Inc.
ABA (Wires): 026 009 593
SWIFT: BOFAUS3N
Account: 3756319819

Send checks to:
Motorola Solutions, Inc.
13104 Collections Center Drive
Chicago, IL 60693
USA
Remittance: US.remittance@motorolasolutions.com

Payment Inquiries: Vesta.AccountsReceivable@motorolasolutions.com
+1 (951) 719-2230



CERTIFICATE OF LIABILITY INSURANCE

DATE(MM/DD/YYYY)
06/18/2020

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER
Aon Risk Services Central, Inc.
Chicago IL Office
200 East Randolph
Chicago IL 60601 USA

CONTACT
NAME:
PHONE
(A/C. No. Ext): (866) 283-7122 FAX
(A/C. No.): (800) 363-0105
E-MAIL
ADDRESS:

INSURED
Motorola Solutions, Inc.
Attn Karen Napier
500 West Monroe
Chicago IL 60661 USA

INSURER(S) AFFORDING COVERAGE		NAIC #
INSURER A:	Liberty Mutual Fire Ins Co	23035
INSURER B:	Liberty Insurance Corporation	42404
INSURER C:	Lloyd's Syndicate No. 4711	AA1120090
INSURER D:		
INSURER E:		
INSURER F:		

COVERAGES

CERTIFICATE NUMBER: 570082412685

REVISION NUMBER:

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

Limits shown are as requested

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS
A	<input checked="" type="checkbox"/> COMMERCIAL GENERAL LIABILITY <input type="checkbox"/> CLAIMS-MADE <input checked="" type="checkbox"/> OCCUR GEN'L AGGREGATE LIMIT APPLIES PER: <input checked="" type="checkbox"/> POLICY <input type="checkbox"/> PRO-JECT <input type="checkbox"/> LOC OTHER:			TB2641005169070	07/01/2020	07/01/2021	EACH OCCURRENCE \$2,000,000 DAMAGE TO RENTED PREMISES (Ea occurrence) \$250,000 MED EXP (Any one person) \$10,000 PERSONAL & ADV INJURY \$2,000,000 GENERAL AGGREGATE \$3,000,000 PRODUCTS - COMP/OP AGG \$2,000,000
A	<input checked="" type="checkbox"/> AUTOMOBILE LIABILITY <input checked="" type="checkbox"/> ANY AUTO <input type="checkbox"/> OWNED AUTOS ONLY <input type="checkbox"/> HIRED AUTOS ONLY <input type="checkbox"/> SCHEDULED AUTOS <input type="checkbox"/> NON-OWNED AUTOS ONLY			AS2-641-005169-010	07/01/2020	07/01/2021	COMBINED SINGLE LIMIT (Ea accident) \$2,000,000 BODILY INJURY (Per person) BODILY INJURY (Per accident) PROPERTY DAMAGE (Per accident)
	<input type="checkbox"/> UMBRELLA LIAB <input type="checkbox"/> OCCUR <input type="checkbox"/> EXCESS LIAB <input type="checkbox"/> CLAIMS-MADE <input type="checkbox"/> DED <input type="checkbox"/> RETENTION						EACH OCCURRENCE AGGREGATE
B	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY ANY PROPRIETOR / PARTNER / EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NM) If yes, describe under DESCRIPTION OF OPERATIONS below	Y/N N	N/A	WA764B005169080 All Other States WC7641005169090 WI	07/01/2020	07/01/2021	<input checked="" type="checkbox"/> PER STATUTE <input type="checkbox"/> OTHER E.L. EACH ACCIDENT \$1,000,000 E.L. DISEASE-EA EMPLOYEE \$1,000,000 E.L. DISEASE-POLICY LIMIT \$1,000,000
C	E&O-MPL-Primary			FSCE02000661	07/01/2020	07/01/2021	Each Claim \$2,000,000 Policy Aggregate \$2,000,000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

Evidence of Insurance.

CERTIFICATE HOLDER

Motorola Solutions, Inc.
500 W. Monroe
Chicago IL 60661 USA

CANCELLATION

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE

Aon Risk Services Central, Inc.

Holder Identifier :

Certificate No : 570082412685



Nicholas A. Toumpas
Commissioner

Marcella J. Bobinsky
Acting Director

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES

29 HAZEN DRIVE, CONCORD, NH 03301-6527
603-271-4741 1-800-852-3345 Ext. 4741
Fax: 603-271-4506 TDD Access: 1-800-735-2964



September 17, 2015

Her Excellency, Governor Margaret Wood Hassan
and the Honorable Council
State House
Concord, New Hampshire 03301

Sole Source

REQUESTED ACTION

Authorize the Department of Health and Human Services, Division of Public Health Services, to enter into a **sole source** agreement with Airbus DS Communications, Inc. (Vendor #207537), 117 Seaboard Lane, Suite D-100, Franklin, TN 37067, for the provision of transitional services to move the hosting of the Communicator NXT System, from in-house hosting to Vendor hosting, and to provide continued maintenance, and support services of the System, in an amount not to exceed \$198,950, to be effective date of Governor and Council approval through August 31, 2020. The source of funding is 100% Federal Funds.

Funding to support this request is anticipated to be available in the following accounts in State Fiscal Years 2016, 2017, 2018, 2019, 2020, and 2021 upon the availability and continued appropriation of funds in future operating budgets, with authority to adjust encumbrances between State Fiscal Years, through the Budget Office, without further approval from Governor and Executive Council, if needed and justified.

05-95-90-902510-5084, HEALTH AND SOCIAL SERVICES, DEPT OF HEALTH AND HUMAN SERVICES, HHS: DIVISION OF PUBLIC HEALTH, BUREAU OF INFECTIOUS DISEASE CONTROL, EBOLA GRANT

Fiscal Year	Class/Object	Class Title	Job Number	Total Amount
SFY 2016	102-500731	Contracts for Prog Svc.	90027030	\$33,208
SFY 2017	102-500731	Contracts for Prog Svc.	90027030	\$6,642
			Sub-Total	\$39,850

05-95-90-902510-7545, HEALTH AND SOCIAL SERVICES, DEPT OF HEALTH AND HUMAN SERVICES, HHS: DIVISION OF PUBLIC HEALTH, BUREAU OF INFECTIOUS DISEASE CONTROL, EMERGENCY PREPAREDNESS

Fiscal Year	Class/Object	Class Title	Job Number	Total Amount
SFY 2017	102-500731	Contracts for Prog Svc.	90077002	\$35,458
SFY 2018	102-500731	Contracts for Prog Svc.	90077002	\$39,467
SFY 2019	102-500731	Contracts for Prog Svc.	90077002	\$38,850
SFY 2020	102-500731	Contracts for Prog Svc.	90077002	\$38,850
SFY 2021	102-500731	Contracts for Prog Svc.	90077002	\$6,475
			Sub-Total	\$159,100
			Total	\$198,950

EXPLANATION

This **sole source** request is being made because the vendor, Airbus DS Communications, Inc. is uniquely qualified to host and support the Communicator NXT System as they have provided maintenance, support, and back up services to the State for the in-house hosted hardware and software for the Communicator NXT System since 2002. No other vendor would be able to take over the hosting and maintenance of this proprietary System.

The system was last upgraded in June 2009 and is currently due for an upgrade to Version 4.4.2. This upgrade would require the replacement of 2 physical servers in the in-house hosting environment, (due to the use of 24 phone lines). As an alternative to upgrading servers, the Department has determined that using the Airbus-hosted option will eliminate the need to upgrade local servers and will provide the same level of access to the notification system, at a savings of \$12,000 per year for the duration of the contract term for a total cost savings of approximately \$66,000.

Funds in this agreement will be used to transition the hosting of the Communicator NXT System from an in-house hosted environment to a Vendor-hosted environment and for the continued support and maintenance of the System software. The Communicator NXT System is a web-based, high-speed notification system used by DPHS and other internal and external partners to communicate with appropriate health professionals, agencies and institutions in the event of a public health alert or advisory. The System is used to send out approximately 20 – 30 health alerts each year as well as activate the Public Health Incident Management Team during emergencies.

As referenced in Part 2, Exhibit C, Special Provisions, this Agreement has the option to extend for four (4) additional years, contingent upon satisfactory delivery of services, available funding, agreement of the parties and approval of the Governor and Council.

The following performance measures will be used to measure the effectiveness of the agreement.

1. The Final Work Plan is accepted by the State.
2. The mapping of the legacy Data to the Airbus application as specified in Contract 2015-049 Part 3.
3. New System in place and ready to use as primary system 20 days after contract approval.

4. New System is running ten (10) weeks after contract approval.
5. Annual comprehensive web-based training will be conducted for ten (10) DHHS staff members per contract year.
6. System down-time is less than 1% per year.
7. Warranty Period is completed as defined in Contract 2015-049 Part 3.

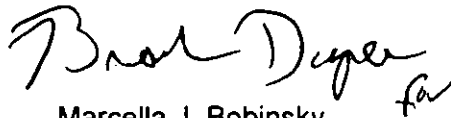
Should Governor and Executive Council not authorize this Request, the State will lose its alerting and notification system while the State sought alternatives, undoubtedly at a higher cost.

Area served: Statewide.

Source of Funds: 100% Federal Funds from the Centers for Disease Control and Prevention, Coordinating Office for Terrorism Preparedness & Emergency Response, Catalog of Federal and Domestic Assistance Number, 93.074, Federal Award Identification Number (FAIN) #U90TP000535.

In the event that the Federal Funds become no longer available, General Funds will not be requested to support this program.

Respectfully submitted,



Marcella J. Bobinsky
Acting Director

Approved by:



Nicholas A. Toupas
Commissioner



STATE OF NEW HAMPSHIRE
DEPARTMENT OF INFORMATION TECHNOLOGY
27 Hazen Dr., Concord, NH 03301
Fax: 603-271-1516 TDD Access: 1-800-735-2964
www.nh.gov/doit

Denis Goulet
Commissioner

August 24, 2015

Nicholas Toumpas, Commissioner
State of New Hampshire
Department of Health and Human Services
129 Pleasant Street
Concord, NH 03301-3857

Dear Commissioner Toumpas:

This letter represents formal notification that the Department of Information Technology (DoIT) has approved your agency's request to enter into a **sole source** contract with Airbus DS Communications, Inc. as described below and referenced as DoIT No. 2015-049.

The purpose of this contract is to provide maintenance, support, and backup services by Airbus DS Communications. The Communicator NXT system is a web-based high-speed notification system used by Divisions of Public Health Services and other internal and external partners. The contract with Airbus will achieve cost savings and maintain existing alerting capacity because Airbus has been the exclusive vendor since 2002 for providing maintenance, support, and backup services. The funding amount is not to exceed \$198,950, and the contract shall become effective upon Governor and Council Approval and expire on August 31, 2021.

A copy of this letter should accompany the Department of Health and Human Services' submission to the Governor and Executive Council for approval.

Sincerely,

A handwritten signature in black ink, appearing to read "Denis Goulet", with a stylized flourish at the end.

Denis Goulet

DG/mh
Contract 2015-049

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
AIRBUS DS COMMUNICATIONS
CONTRACT 2015-049
AGREEMENT- PART 1

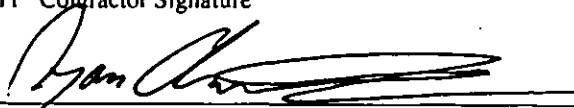
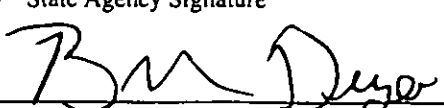
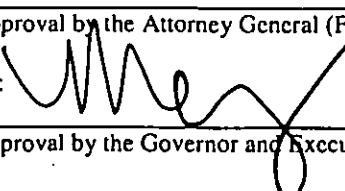
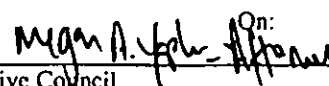
Subject: Communicator Hosting, Maintenance and Support Services

AGREEMENT

The State of New Hampshire and the Contractor hereby mutually agree as follows:

GENERAL PROVISIONS

1. IDENTIFICATION.

1.1 State Agency Name Department of Health and Human Services		1.2 State Agency Address 129 Pleasant Street Concord, NH 03301-3857	
1.3 Contractor Name Airbus DS Communications, Inc.		1.4 Contractor Address 117 Seaboard Lane, Suite D-100 Franklin, TN 37067	
1.5 Contractor Phone Number 615-790-2882	1.6 05-95-90-902510-5084-102-500731 05-95-90-902510-7545-102-500731	1.7 Completion Date 8/31/2020	1.8 Price Limitation \$198,950
1.9 Contracting Officer for State Agency Brook Dupee		1.10 State Agency Telephone Number 603-271-4483	
1.11 Contractor Signature 		1.11 Name and Title of Contractor Signatory Ryan Christensen, Legal Counsel	
1.12 Acknowledgement: State of Tennessee, County of Franklin On _____, before the undersigned officer, personally appeared the person identified in block 1.12, or satisfactorily proven to be the person whose name is signed in block 1.11, and acknowledged that s/he executed this document in the capacity indicated in block 1.12.			
1.13.1 Signature of Notary Public or Justice of the Peace <div style="text-align: right; font-style: italic;">See attached notarization</div>			
1.13.2 Name and Title of Notary or Justice of the Peace			
1.14 State Agency Signature 		1.15 Name and Title of State Agency Signatory Brook S. Dupa / Bureau Chief	
1.16 Approval by the N.H. Department of Administration, Division of Personnel (if applicable) By: _____ Director, On: _____			
1.17 Approval by the Attorney General (Form, Substance and Execution) By:  On:  9/13/15			
1.18 Approval by the Governor and Executive Council By: _____ On: _____			

ACKNOWLEDGMENT

A notary public or other officer completing this certificate verifies only the identity of the individual who signed the document to which this certificate is attached, and not the truthfulness, accuracy, or validity of that document.

State of California
County of RIVERSIDE

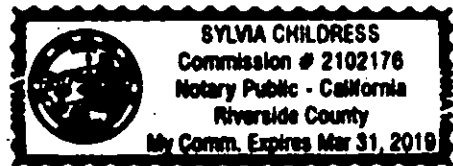
On July 21, 2015 before me, SYLVIA CHILDRESS, Notary Public,
(insert name and title of the officer)

personally appeared Ryan T. Christensen
who proved to me on the basis of satisfactory evidence to be the person~~s~~ whose name~~s~~ ~~is~~ are
subscribed to the within instrument and acknowledged to me that ~~he~~/she/they executed the same in
~~his~~/her/their authorized capacity~~(ies)~~, and that by ~~his~~/her/their signature~~s~~ on the instrument the
person~~s~~, or the entity upon behalf of which the person~~s~~ acted, executed the instrument.

I certify under PENALTY OF PERJURY under the laws of the State of California that the foregoing paragraph is true and correct.

WITNESS my hand and official seal.

Signature Sylvia Childress (Seal)



2. EMPLOYMENT OF CONTRACTOR/SERVICES TO BE PERFORMED. The State of New Hampshire, acting through the agency identified in block 1.1 ("State"), engages contractor identified in block 1.3 ("Contractor") to perform, and the Contractor shall perform, the work or sale of goods, or both, identified and more particularly described in the attached EXHIBIT A which is incorporated herein by reference ("Services").

3. EFFECTIVE DATE/COMPLETION OF SERVICES.

3.1 Notwithstanding any provision of this Agreement to the contrary, and subject to the approval of the Governor and Executive Council of the State of New Hampshire, this Agreement, and all obligations of the parties hereunder, shall not become effective until the date the Governor and Executive Council approve this Agreement ("Effective Date").
3.2 If the Contractor commences the Services prior to the Effective Date, all Services performed by the Contractor prior to the Effective Date shall be performed at the sole risk of the Contractor, and in the event that this Agreement does not become effective, the State shall have no liability to the Contractor, including without limitation, any obligation to pay the Contractor for any costs incurred or Services performed. Contractor must complete all Services by the Completion Date specified in block 1.7.

4. CONDITIONAL NATURE OF AGREEMENT.

Notwithstanding any provision of this Agreement to the contrary, all obligations of the State hereunder, including, without limitation, the continuance of payments hereunder, are contingent upon the availability and continued appropriation of funds, and in no event shall the State be liable for any payments hereunder in excess of such available appropriated funds. In the event of a reduction or termination of appropriated funds, the State shall have the right to withhold payment until such funds become available, if ever, and shall have the right to terminate this Agreement immediately upon giving the Contractor notice of such termination. The State shall not be required to transfer funds from any other account to the Account identified in block 1.6 in the event funds in that Account are reduced or unavailable.

5. CONTRACT PRICE/PRICE LIMITATION/PAYMENT.

5.1 The contract price, method of payment, and terms of payment are identified and more particularly described in EXHIBIT B which is incorporated herein by reference.
5.2 The payment by the State of the contract price shall be the only and the complete reimbursement to the Contractor for all expenses, of whatever nature incurred by the Contractor in the performance hereof, and shall be the only and the complete compensation to the Contractor for the Services. The State shall have no liability to the Contractor other than the contract price.
5.3 The State reserves the right to offset from any amounts otherwise payable to the Contractor under this Agreement

those liquidated amounts required or permitted by N.H. RSA 80:7 through RSA 80:7-c or any other provision of law.

5.4 Notwithstanding any provision in this Agreement to the contrary, and notwithstanding unexpected circumstances, in no event shall the total of all payments authorized, or actually made hereunder, exceed the Price Limitation set forth in block 1.8.

6. COMPLIANCE BY CONTRACTOR WITH LAWS AND REGULATIONS/ EQUAL EMPLOYMENT OPPORTUNITY.

6.1 In connection with the performance of the Services, the Contractor shall comply with all statutes, laws, regulations, and orders of federal, state, county or municipal authorities which impose any obligation or duty upon the Contractor, including, but not limited to, civil rights and equal opportunity laws. In addition, the Contractor shall comply with all applicable copyright laws.

6.2 During the term of this Agreement, the Contractor shall not discriminate against employees or applicants for employment because of race, color, religion, creed, age, sex, handicap, sexual orientation, or national origin and will take affirmative action to prevent such discrimination.

6.3 If this Agreement is funded in any part by monies of the United States, the Contractor shall comply with all the provisions of Executive Order No. 11246 ("Equal Employment Opportunity"), as supplemented by the regulations of the United States Department of Labor (41 C.F.R. Part 60), and with any rules, regulations and guidelines as the State of New Hampshire or the United States issue to implement these regulations. The Contractor further agrees to permit the State or United States access to any of the Contractor's books, records and accounts for the purpose of ascertaining compliance with all rules, regulations and orders, and the covenants, terms and conditions of this Agreement.

7. PERSONNEL.

7.1 The Contractor shall at its own expense provide all personnel necessary to perform the Services. The Contractor warrants that all personnel engaged in the Services shall be qualified to perform the Services, and shall be properly licensed and otherwise authorized to do so under all applicable laws.

7.2 Unless otherwise authorized in writing, during the term of this Agreement, and for a period of six (6) months after the Completion Date in block 1.7, the Contractor shall not hire, and shall not permit any subcontractor or other person, firm or corporation with whom it is engaged in a combined effort to perform the Services to hire, any person who is a State employee or official, who is materially involved in the procurement, administration or performance of this Agreement. This provision shall survive termination of this Agreement.

7.3 The Contracting Officer specified in block 1.9, or his or her successor, shall be the State's representative. In the event of any dispute concerning the interpretation of this Agreement, the Contracting Officer's decision shall be final for the State.

8. EVENT OF DEFAULT/REMEDIES.

8.1 Any one or more of the following acts or omissions of the Contractor shall constitute an event of default hereunder ("Event of Default"):

8.1.1 failure to perform the Services satisfactorily or on schedule;

8.1.2 failure to submit any report required hereunder; and/or

8.1.3 failure to perform any other covenant, term or condition of this Agreement.

8.2 Upon the occurrence of any Event of Default, the State may take any one, or more, or all, of the following actions:

8.2.1 give the Contractor a written notice specifying the Event of Default and requiring it to be remedied within, in the absence of a greater or lesser specification of time, thirty (30) days from the date of the notice; and if the Event of Default is not timely remedied, terminate this Agreement, effective two (2) days after giving the Contractor notice of termination;

8.2.2 give the Contractor a written notice specifying the Event of Default and suspending all payments to be made under this Agreement and ordering that the portion of the contract price which would otherwise accrue to the Contractor during the period from the date of such notice until such time as the State determines that the Contractor has cured the Event of Default shall never be paid to the Contractor;

8.2.3 set off against any other obligations the State may owe to the Contractor any damages the State suffers by reason of any Event of Default; and/or

8.2.4 treat the Agreement as breached and pursue any of its remedies at law or in equity, or both.

9. DATA/ACCESS/CONFIDENTIALITY/PRESERVATION.

9.1 As used in this Agreement, the word "data" shall mean all information and things developed or obtained during the performance of, or acquired or developed by reason of, this Agreement, including, but not limited to, all studies, reports, files, formulae, surveys, maps, charts, sound recordings, video recordings, pictorial reproductions, drawings, analyses, graphic representations, computer programs, computer printouts, notes, letters, memoranda, papers, and documents, all whether finished or unfinished.

9.2 All data and any property which has been received from the State or purchased with funds provided for that purpose under this Agreement, shall be the property of the State, and shall be returned to the State upon demand or upon termination of this Agreement for any reason.

9.3 Confidentiality of data shall be governed by N.H. RSA chapter 91-A or other existing law. Disclosure of data requires prior written approval of the State.

10. TERMINATION. In the event of an early termination of this Agreement for any reason other than the completion of the Services, the Contractor shall deliver to the Contracting Officer, not later than fifteen (15) days after the date of

termination, a report ("Termination Report") describing in detail all Services performed, and the contract price earned, to and including the date of termination. The form, subject matter, content, and number of copies of the Termination Report shall be identical to those of any Final Report described in the attached EXHIBIT A.

11. CONTRACTOR'S RELATION TO THE STATE. In the performance of this Agreement the Contractor is in all respects an independent contractor, and is neither an agent nor an employee of the State. Neither the Contractor nor any of its officers, employees, agents or members shall have authority to bind the State or receive any benefits, workers' compensation or other emoluments provided by the State to its employees.

12. ASSIGNMENT/DELEGATION/SUBCONTRACTS.

The Contractor shall not assign, or otherwise transfer any interest in this Agreement without the prior written consent of the N.H. Department of Administrative Services. None of the Services shall be subcontracted by the Contractor without the prior written consent of the State.

13. INDEMNIFICATION. The Contractor shall defend, indemnify and hold harmless the State, its officers and employees, from and against any and all losses suffered by the State, its officers and employees, and any and all claims, liabilities or penalties asserted against the State, its officers and employees, by or on behalf of any person, on account of, based or resulting from, arising out of (or which may be claimed to arise out of) the acts or omissions of the Contractor. Notwithstanding the foregoing, nothing herein contained shall be deemed to constitute a waiver of the sovereign immunity of the State, which immunity is hereby reserved to the State. This covenant in paragraph 13 shall survive the termination of this Agreement.

14. INSURANCE.

14.1 The Contractor shall, at its sole expense, obtain and maintain in force, and shall require any subcontractor or assignee to obtain and maintain in force, the following insurance:

14.1.1 comprehensive general liability insurance against all claims of bodily injury, death or property damage, in amounts of not less than \$250,000 per claim and \$2,000,000 per occurrence; and

14.1.2 fire and extended coverage insurance covering all property subject to subparagraph 9.2 herein, in an amount not less than 80% of the whole replacement value of the property.

14.2 The policies described in subparagraph 14.1 herein shall be on policy forms and endorsements approved for use in the State of New Hampshire by the N.H. Department of Insurance, and issued by insurers licensed in the State of New Hampshire.

14.3 The Contractor shall furnish to the Contracting Officer identified in block 1.9, or his or her successor, a certificate(s) of insurance for all insurance required under this Agreement. Contractor shall also furnish to the Contracting Officer

identified in block 1.9, or his or her successor, certificate(s) of insurance for all renewal(s) of insurance required under this Agreement no later than fifteen (15) days prior to the expiration date of each of the insurance policies. The certificate(s) of insurance and any renewals thereof shall be attached and are incorporated herein by reference. Each certificate(s) of insurance shall contain a clause requiring the insurer to endeavor to provide the Contracting Officer identified in block 1.9, or his or her successor, no less than ten (10) days prior written notice of cancellation or modification of the policy.

15. WORKERS' COMPENSATION.

15.1 By signing this agreement, the Contractor agrees, certifies and warrants that the Contractor is in compliance with or exempt from, the requirements of N.H. RSA chapter 281-A ("*Workers' Compensation*").

15.2 To the extent the Contractor is subject to the requirements of N.H. RSA chapter 281-A, Contractor shall maintain, and require any subcontractor or assignee to secure and maintain, payment of Workers' Compensation in connection with activities which the person proposes to undertake pursuant to this Agreement. Contractor shall furnish the Contracting Officer identified in block 1.9, or his or her successor, proof of Workers' Compensation in the manner described in N.H. RSA chapter 281-A and any applicable renewal(s) thereof, which shall be attached and are incorporated herein by reference. The State shall not be responsible for payment of any Workers' Compensation premiums or for any other claim or benefit for Contractor, or any subcontractor or employee of Contractor, which might arise under applicable State of New Hampshire Workers' Compensation laws in connection with the performance of the Services under this Agreement.

16. WAIVER OF BREACH. No failure by the State to enforce any provisions hereof after any Event of Default shall be deemed a waiver of its rights with regard to that Event of Default, or any subsequent Event of Default. No express failure to enforce any Event of Default shall be deemed a waiver of the right of the State to enforce each and all of the provisions hereof upon any further or other Event of Default on the part of the Contractor.

17. NOTICE. Any notice by a party hereto to the other party shall be deemed to have been duly delivered or given at the time of mailing by certified mail, postage prepaid, in a United States Post Office addressed to the parties at the addresses given in blocks 1.2 and 1.4, herein.

18. AMENDMENT. This Agreement may be amended, waived or discharged only by an instrument in writing signed by the parties hereto and only after approval of such amendment, waiver or discharge by the Governor and Executive Council of the State of New Hampshire.

19. CONSTRUCTION OF AGREEMENT AND TERMS.

This Agreement shall be construed in accordance with the laws of the State of New Hampshire, and is binding upon and inures to the benefit of the parties and their respective successors and assigns. The wording used in this Agreement is the wording chosen by the parties to express their mutual intent, and no rule of construction shall be applied against or in favor of any party.

20. THIRD PARTIES. The parties hereto do not intend to benefit any third parties and this Agreement shall not be construed to confer any such benefit.

21. HEADINGS. The headings throughout the Agreement are for reference purposes only, and the words contained therein shall in no way be held to explain, modify, amplify or aid in the interpretation, construction or meaning of the provisions of this Agreement.

22. SPECIAL PROVISIONS. Additional provisions set forth in the attached EXHIBIT C are incorporated herein by reference.

23. SEVERABILITY. In the event any of the provisions of this Agreement are held by a court of competent jurisdiction to be contrary to any state or federal law, the remaining provisions of this Agreement will remain in full force and effect.

24. ENTIRE AGREEMENT. This Agreement, which may be executed in a number of counterparts, each of which shall be deemed an original, constitutes the entire Agreement and understanding between the parties, and supersedes all prior Agreements and understandings relating hereto.

**STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT - PART 2**

INTRODUCTION

This Contract is by and between the State of New Hampshire, acting through the Department of Health and Human Services (DHHS) ("State"), and Airbus DS Communications, Inc. a Tennessee Corporation, ("Airbus") having its principal place of business at 117 Seaboard Lane, Suite D-100, Franklin, TN 37067

This contract will provide transitional services required to move the hosting of the Communicator Software from in-house hosting to Airbus DS Communications, Inc. hosting, as well as continued maintenance, and support services for the Software. The Communicator is a web-based high-speed notification system used by DHHS and other internal and external partners. The System is used to communicate with appropriate persons in the event of a health alert or advisory.

RECITALS

The State desires to have Airbus DS Communications, Inc. provide Software as a Service (SaaS) for the DHHS;

Airbus DS Communications wishes to provide Software as a Service (SaaS) for the State.

The parties therefore agree as follows:

1. CONTRACT DOCUMENTS

1.1 Contract Documents

This Contract is comprised of the following documents (Contract Documents):

- A. Part 1 – State Terms and Conditions contained in the Form P-37
- B. Part 2 – The Contract Agreement
- C. Part 3 – Consolidated Exhibits
 - Exhibit A - Contract Deliverables
 - Exhibit B - Price and Payment Schedule
 - Exhibit C - Special Provisions
 - Exhibit D - Administrative Services
 - Exhibit E - Implementation Services
 - Exhibit E.1 – Security and Infrastructure
 - Exhibit F - Testing Services
 - Exhibit G - Maintenance and Support Services
 - Exhibit H - Requirements
 - Exhibit I - Work Plan
 - Exhibit J - Software License and related Terms
 - Exhibit K - Warranty and Warranty Services
 - Exhibit L - Training Services
 - Exhibit M - Reserved
 - Exhibit N - Airbus Proposal, by reference

Contract 2015-049 Agreement-Part 2

Initial and Date All Pages:

Airbus initials: AC

Date: 7-21-2015

**STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT – PART 2**

Exhibit O – Special Exhibits, Attachments and Certificates

1.2 Order of Precedence

In the event of conflict or ambiguity among any of the text of the Contract Documents, the following Order of Precedence shall govern:

- a. *The State of New Hampshire Terms and Conditions*, Form P-37-Contract Agreement Part I
- b. State of New Hampshire, DHHS Contract 2015-049 Part 2.
- c. The Terms and conditions set forth in the Consolidated Exhibits A-N.

2. COMPENSATION

2.1 Contract Price

The Contract price, method of payment, and terms of payment are identified and more particularly described in Contract Exhibit B: *Price and Payment Schedule*.

2.2 Non-Exclusive, Not to Exceed Contract

This is a Non-Exclusive, Not to Exceed (NTE) Contract with price and term limitations as set forth in the Contract.

The State reserves the right, at its discretion, to retain other contractors to provide any of the Services or Deliverables identified under this procurement or make an award by item, part or portion of an item, group of items, or total Proposal. Airbus shall not be responsible for any delay, act, or omission of such other contractors, except that Airbus shall be responsible for any delay, act, or omission of the other contractors if such delay, act, or omission is caused by or due to the fault of Airbus.

3. CONTRACT MANAGEMENT

The Project will require the coordinated efforts of a Project Team consisting of both Airbus and State personnel. Airbus shall provide all necessary resources to perform its obligations under the Contract. Airbus shall be responsible for managing the Project to its successful completion.

3.1 Airbus's Contract Manager

Airbus shall assign a Contract Manager who shall be responsible for all Contract authorization and administration. Airbus's Contract Manager is:

Hope Baker
Account Representative
Airbus DS Communications, Inc.
117 Seaboard Lane, Suite D-100
Franklin, TN 37067

Contract 2015-049 Agreement-Part 2

Initial and Date All Pages:

Airbus initials: RC

Date: 7-21-2015

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT – PART 2

Phone: 615.790.2882
Toll-Free: 800.723.3207
Fax: 615.790.1329
Hope.Baker@airbus-dscomm.com

3.2 Airbus's Project Manager

3.2.1 Contract Project Manager

Airbus shall assign a Project Manager who meets the requirements of the Contract, including but not limited to, the requirements set forth in the Contract. Airbus's selection of the Airbus Project Manager shall be subject to the prior written approval of the State. The State's approval process may include, without limitation, at the State's discretion, review of the proposed Airbus Project Manager's resume, qualifications, references, and an interview. The State may require removal or reassignment of Airbus's Project Manager who, in the sole judgment of the State, is found unacceptable or is not performing to the State's satisfaction.

3.2.2 The Airbus Project Manager must be qualified to perform the obligations required of the position under the Contract, shall have full authority to make binding decisions under the Contract, and shall function as Airbus's representative for all administrative and management matters. The Airbus Project Manager shall perform the duties required under the Contract, including, but not limited to, those set forth in Contract Exhibit I, Section 2. The Airbus Project Manager must be available to promptly respond during Normal Business Hours within two (2) hours to inquiries from the State, and be at the site as needed. The Airbus Project Manager must work diligently and use his/ her best efforts on the Project.

3.2.3 Airbus shall not change its assignment of the Airbus Project Manager without providing the State written justification and obtaining the prior written approval of the State. State approvals for replacement of the Airbus's Project Manager shall not be unreasonably withheld. The replacement Project Manager shall have comparable or greater skills than the Airbus Project Manager being replaced; meet the requirements of the Contract; and be subject to reference checks described above in Contract Agreement Part 2, Section 3.2.1: *Contract Project Manager*, and in Contract Agreement Part 2, Section 3.6: *Reference Checks*, below. Airbus shall assign a replacement the Airbus Project Manager within ten (10) business days of the departure of the prior the Airbus Project Manager, and Airbus shall continue during the ten (10) business day period to provide competent Project management Services through the assignment of a qualified interim Project Manager.

3.2.4 Notwithstanding any other provision of the Contract, the State shall have the option, at its discretion, to terminate the Contract, declare Airbus in default and pursue its remedies at law and in equity, if Airbus fails to assign an Airbus Project Manager meeting the requirements and terms of the Contract.

Contract 2015-049 Agreement-Part 2

Initial and Date All Pages:

Airbus initials: RC

Date: 7-21-2015

Page 3 of 28

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT – PART 2

3.2.5 The Airbus Project Manager is:
Frank Hobbs
117 Seaboard Lane, Suite D-100
Franklin, TN 37067

Tel: 615-791-3982
Fax: 615-790-1329
Frank.hobbs@airbus-dscomm.com

3.3 Airbus Key Project Staff

3.3.1 Airbus shall assign Key Project Staff who meet the requirements of the Contract, and can implement the Software Solution meeting the requirements set forth in this Contract. The State may conduct reference checks on Airbus Key Project Staff. The State reserves the right to require removal or reassignment of Airbus's Key Project Staff who are found unacceptable to the State.

3.3.2 Airbus shall not change any Airbus Key Project Staff commitments without providing the State written justification and obtaining the prior written approval of the State. State approvals for replacement of Airbus Key Project Staff will not be unreasonably withheld. The replacement Airbus Key Project Staff shall have comparable or greater skills than Airbus Key Project Staff being replaced; meet the requirements of the Contract and be subject to reference checks described in Contract Agreement-Part 2, Section 3.6: *Reference Checks*,

3.3.3 Notwithstanding any other provision of the Contract to the contrary, the State shall have the option to terminate the Contract, declare Airbus in default and to pursue its remedies at law and in equity, if Airbus fails to assign Key Project Staff meeting the requirements and terms of the Contract or if it is dissatisfied with Airbus's replacement Project staff.

3.3.3.1 Airbus Key Project Staff shall consist of the following individuals in the roles identified below:

Airbus's Key Project Staff:

Key Member(s)

Hope Baker
Frank Hobbs

Title

Account Representative
Project Manager

3.4 State Contract Manager

The State shall assign a Contract Manager who shall function as the State's representative with regard to Contract administration. The State Contract Manager is:
Neil Twitchell

**STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT – PART 2**

DHHS – DPHS
Bureau of Public Health Systems Policy and Performance
29 Hazen Drive
Concord, NH 03301
Tel: (603) 271-5194
Email: ntwitchell@dhhs.state.nh.us

3.5 State Project Manager

The State shall assign a Project Manager. The State Project Manager's duties shall include the following:

- a. Leading the Project;
- b. Engaging and managing all the Contracted Vendors;
- c. Managing significant issues and risks.
- d. Reviewing and accepting Contract Deliverables;
- e. Invoice sign-offs;
- f. Review and approval of change proposals; and
- g. Managing stakeholders' concerns

The State Project Manager is:
Thomas Flynn
DHHS – DPHS
Bureau of Public Health Systems Policy and Performance
29 Hazen Drive
Concord, NH 03301
Tel: (603) 271-7499
Email: tdflynn@dhhs.state.nh.us

3.6 Reference Checks

The State may, at its sole expense, conduct reference screening of Airbus Project Manager and Airbus Key Project Staff.

4. DELIVERABLES

4.1 Airbus Responsibilities

Airbus shall be solely responsible for meeting all requirements, and terms and conditions specified in this Contract, regardless of whether or not a Subcontractor is used.

Airbus may subcontract Services subject to the provisions of the Contract. Airbus must submit all information and documentation relating to the Subcontractor, including terms and conditions consistent with this Contract. The State will consider Airbus to be wholly responsible for the performance of the Contract and the sole point of contact with regard to all contractual matters, including payment of any and all charges resulting from the Contract.

Contract 2015-049 Agreement-Part 2

Initial and Date All Pages:

Airbus initials: AC

Date: 7-21-2015

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT – PART 2

4.2 Deliverables and Services

Airbus shall provide the State with the Deliverables and Services in accordance with the time frames in the Work Plan for this Contract, and as more particularly described in Contract Exhibit A: *Contract Deliverables*.

Upon its submission of a Deliverable or Service, Airbus represents that it has performed its obligations under the Contract associated with the Deliverable or Service.

4.3 Non-Software and Written Deliverables Review and Acceptance

After receiving written Certification from Airbus that a Non-Software or Written Deliverable is final, complete, and ready for Review, the State will Review the Deliverable to determine whether it meets the specifications outlined in the contract. The State will notify Airbus in writing of its Acceptance or rejection of the Deliverable within five (5) business days of the State's receipt of Airbus's written Certification. If the State rejects the Deliverable, the State shall notify Airbus of the nature and class of the Deficiency and Airbus shall correct the Deficiency within the period identified in the Work Plan. If no period for Airbus's correction of the Deliverable is identified, Airbus shall correct the Deficiency in the Deliverable within five (5) business days. Upon receipt of the corrected Deliverable, the State shall have five (5) business days to review the Deliverable and notify Airbus of its Acceptance or rejection thereof, with the option to extend the Review Period up to five (5) additional business days. If Airbus fails to correct the Deficiency within the allotted period of time, the State may, at its option, continue reviewing the Deliverable and require Airbus to continue until the Deficiency is corrected, or immediately terminate the Contract, declare Airbus in default, and pursue its remedies at law and in equity.

4.4 System/Software Testing and Acceptance

System/Software Testing and Acceptance shall be performed as set forth in the Test Plan and more particularly described in Exhibit F: *Testing Services*.

4.5 Security

The State must ensure that appropriate levels of security are implemented and maintained in order to protect the integrity and reliability of its information technology resources, information, and services. State resources, information, and services must be available on an ongoing basis, with the appropriate infrastructure and security controls to ensure business continuity and safeguard State networks, Systems and Data.

IT Security involves all functions pertaining to the securing of State Data and Systems through the creation and definition of security policies, procedures and controls covering such areas as identification, authentication and non-repudiation.

All components of the Software shall be reviewed and tested to ensure they protect the State's hardware and software and its related Data assets. See *Contract Agreement – Part 3 – Exhibit F: Testing* for detailed information on requirements for Security testing.

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT – PART 2

5. SOFTWARE

5.1 Title

Airbus must hold the right to allow the State to use the Software or hold all title, right, and interest in the Software and its associated Documentation.

5.2 Restrictions

Except as otherwise permitted under the Contract, the State agrees not to:

- a. Remove or modify any program markings or any notice of Airbus's proprietary rights;
- b. Make the programs or materials available in any manner to any third party for use in the third party's business operations, except as permitted herein; or
- c. Cause or permit reverse engineering, disassembly or recompilation of the programs.

6. WARRANTY

Airbus shall provide the Warranty and Warranty Services set forth in the Contract, and particularly described in Exhibit K: *Warranty and Warranty Services*.

7. SERVICES

Airbus shall provide the Services required under the Contract Documents. All Services shall meet, and be performed, in accordance with the Specifications.

7.1 Administrative Services

Airbus shall provide the State with the administrative Services set forth in the Contract, and particularly described in Exhibit D: *Administrative Services*.

7.2 Implementation Services

Airbus shall provide the State with the Implementation Services set forth in the Contract, and particularly described in Exhibit E: *Implementation Services*.

7.3 Testing Services

Airbus shall perform testing Services for the State set forth in the Contract, and particularly described in Exhibit F: *Testing Services*.

7.4 Training Services

Airbus shall provide the State with training Services set forth in the Contract, and particularly described in Exhibit L: *Training Services*.

7.5 Maintenance and Support Services

Airbus shall provide the State with Maintenance and support Services for the Software set forth in the Contract, and particularly described in Exhibit G: *System Maintenance and Support*.

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT – PART 2

8. WORK PLAN DELIVERABLE

Airbus shall provide the State with a Work Plan that shall include, without limitation, a detailed description of the Schedule, tasks, Deliverables, major milestones, task dependencies, and payment Schedule.

The initial Work Plan shall be a separate Deliverable and is set forth in Contract Exhibit I: *Work Plan*. Airbus shall update the Work Plan as necessary, but no less than every two weeks, to accurately reflect the status of the Project, including without limitation, the Schedule, tasks, Deliverables, major milestones, task dependencies, and payment Schedule. Any such updates to the Work Plan must be approved by the State, in writing, prior to final incorporation into Contract Exhibit I: *Work Plan*. The updated Contract Exhibit I: *Work Plan*, as approved by the State, is incorporated herein by reference.

Unless otherwise agreed in writing by the State, changes to the Contract Exhibit I: *Work Plan* shall not relieve Airbus from liability to the State for damages resulting from Airbus's failure to perform its obligations under the Contract, including, without limitation, performance in accordance with the Schedule.

In the event of any delay in the Schedule, Airbus must immediately notify the State in writing, identifying the nature of the delay, i.e., specific actions or inactions of Airbus or the State causing the problem; its estimated duration period to reconciliation; specific actions that need to be taken to correct the problem; and the expected Schedule impact on the Project.

In the event additional time is required by Airbus to correct Deficiencies, the Schedule shall not change unless previously agreed in writing by the State, except that the Schedule shall automatically extend on a day-to-day basis to the extent that the delay does not result from Airbus's failure to fulfill its obligations under the Contract. To the extent that the State's execution of its major tasks takes longer than described in the Work Plan, the Schedule shall automatically extend on a day-to-day basis.

Notwithstanding anything to the contrary, the State shall have the option to terminate the Contract for default, at its discretion, if it is dissatisfied with Airbus's Work Plan or elements within the Work Plan.

9. CHANGE ORDERS

The State may make changes or revisions at any time by written Change Order. The State originated changes or revisions shall be approved by the Department of Information Technology (DoIT). Within five (5) business days of Airbus's receipt of a Change Order, Airbus shall advise the State, in detail, of any impact on cost (e.g., increase or decrease), the Schedule, or the Work Plan.

Airbus may request a change within the scope of the Contract by written Change Order, identifying any impact on cost, the Schedule, or the Work Plan. The State shall attempt to respond to Airbus's requested Change Order within five (5) business days. The State Agency, as

**STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT – PART 2**

well as the DoIT, must approve all Change Orders in writing. The State shall be deemed to have rejected the Change Order if the parties are unable to reach an agreement in writing.

All Change Order requests from Airbus to the State, and the State acceptance of Airbus's estimate for a State requested change, will be acknowledged and responded to, either acceptance or rejection, in writing. If accepted, the Change Order(s) shall be subject to the Contract amendment process, as determined to apply by the State.

10. INTELLECTUAL PROPERTY

All title, right, and interest in the Software shall belong to Airbus DS Communications. Upon successful completion and/or termination of the Contract, Airbus shall own and hold all, title, and rights in any Software modifications developed in connection with performance of obligations under the Contract, and the associated Documentation including any and all performance enhancing operational plans and Airbus' special utilities.

In no event shall Airbus be precluded from developing for itself, or for others, materials that are competitive with, or similar to Custom Software, modifications developed in connection with performance of obligations under the Contract. In addition, Airbus shall be free to use its general knowledge, skills, experience, and any other ideas, concepts, know-how, and techniques that are acquired or used in the course of its performance under this agreement.

10.1 State's Data

All rights, title and interest in State Data shall remain with the State.

10.2 Airbus's Materials

Subject to the provisions of this Contract, Airbus may develop for itself, or for others, materials that are competitive with, or similar to, the Deliverables. In accordance with the confidentiality provision of this Contract, Airbus shall not distribute any products containing or disclose any State Confidential Information. Airbus shall be free to use its general knowledge, skills and experience, and any ideas, concepts, know-how, and techniques that are acquired or used in the course of its performance under this Contract, provided that such is not obtained as the result of the deliberate memorization of the State Confidential Information by Airbus employees or third party consultants engaged by Airbus.

Without limiting the foregoing, the parties agree that the general knowledge referred to herein cannot include information or records not subject to public disclosure under New Hampshire RSA Chapter 91-A, which includes but is not limited to the following: records of grand juries and petit juries; records of parole and pardon boards; personal school records of pupils; records pertaining to internal personnel practices, financial information, test questions, scoring keys and other examination data use to administer a licensing examination, examination for employment, or academic examination and personnel, medical, welfare, library use, video tape sale or rental, and other files containing personally identifiable information that is private in nature.

Contract 2015-049 Agreement-Part 2

Initial and Date All Pages:

Airbus initials: HC

Date: 7-21-2015

Page 9 of 28

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT – PART 2

10.3 State Website Copyright

WWW Copyright and Intellectual Property Rights

All right, title and interest in the State WWW site, including copyright to all Data and information, shall remain with the State. The State shall also retain all right, title and interest in any user interfaces and computer instructions embedded within the WWW pages. All WWW pages and any other Data or information shall, where applicable, display the State's copyright.

10.4 Reserved

10.5 Reserved

11. USE OF STATE'S INFORMATION, CONFIDENTIALITY

11.1 Use of State's Information

In performing its obligations under the Contract, Airbus may gain access to information of the State, including State Confidential Information. "State Confidential Information" shall include, but not be limited to, information exempted from public disclosure under New Hampshire RSA Chapter 91-A: *Access to Public Records and Meetings* (see e.g. RSA Chapter 91-A: 5 *Exemptions*). Airbus shall not use the State Confidential Information developed or obtained during the performance of, or acquired, or developed by reason of the Contract, except as directly connected to and necessary for Airbus's performance under the Contract.

11.2 State Confidential Information

Airbus shall maintain the confidentiality of and protect from unauthorized use, disclosure, publication, and reproduction (collectively "release"), all State Confidential Information that becomes available to Airbus in connection with its performance under the Contract, regardless of its form.

Subject to applicable federal or State laws and regulations, Confidential Information shall not include information which: (i) shall have otherwise become publicly available other than as a result of disclosure by the receiving party in breach hereof; (ii) was disclosed to the receiving party on a non-confidential basis from a source other than the disclosing party, which the receiving party believes is not prohibited from disclosing such information as a result of an obligation in favor of the disclosing party; (iii) is developed by the receiving party independently of, or was known by the receiving party prior to, any disclosure of such information made by the disclosing party; or (iv) is disclosed with the written consent of the disclosing party. A receiving party also may disclose Confidential Information to the extent required by an order of a court of competent jurisdiction.

Any disclosure of the State Confidential Information shall require the prior written approval of the State. Airbus shall immediately notify the State if any request, subpoena or other legal process is served upon Airbus regarding the State Confidential Information,

**STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT – PART 2**

and Airbus shall cooperate with the State in any effort the State undertakes to contest the request, subpoena or other legal process, at no additional cost to the State.

In the event of the unauthorized release of State Confidential Information, Airbus shall immediately notify the State, and the State may immediately be entitled to pursue any remedy at law and in equity, including, but not limited to, injunctive relief.

11.3 Airbus Confidential Information

Insofar as Airbus seeks to maintain the confidentiality of its confidential or proprietary information, Airbus must clearly identify in writing all information it claims to be confidential or proprietary. Notwithstanding the foregoing, the State acknowledges that Airbus considers the Software and Documentation to be Confidential Information. Airbus acknowledges that the State is subject to State and federal laws governing disclosure of information including, but not limited to, RSA Chapter 91-A. The State shall maintain the confidentiality of the identified Confidential Information insofar as it is consistent with applicable State and federal laws or regulations, including but not limited to, RSA Chapter 91-A. In the event the State receives a request for the information identified by Airbus as confidential, the State shall notify Airbus and specify the date the State will be releasing the requested information. At the request of the State, Airbus shall cooperate and assist the State with the collection and review of Airbus's information, at no additional expense to the State. Any effort to prohibit or enjoin the release of the information shall be Airbus's sole responsibility and at Airbus's sole expense. If Airbus fails to obtain a court order enjoining the disclosure, the State shall release the information on the date specified in the State's notice to Airbus, without any liability to Airbus.

11.4 Survival

This Contract Agreement Section 11, *Use of State's Information, Confidentiality*, shall survive termination or conclusion of the Contract.

12. LIMITATION OF LIABILITY

12.1 State

Subject to applicable laws and regulations, in no event shall the State be liable for any consequential, special, indirect, incidental, punitive, or exemplary damages. Subject to applicable laws and regulations, the State's liability to Airbus shall not exceed the total Contract price set forth in Contract Agreement, Section 1.8 of the *Contract Agreement – Part 1-General Provisions*.

Notwithstanding the foregoing and any provision of this Contract to the contrary, in no event does the State waive its sovereign immunity or any applicable defenses or immunities.

12.2 Airbus

Contract 2015-049 Agreement-Part 2

Initial and Date All Pages:

Airbus initials: nc
Date: 7-21-2015

Page 11 of 28

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT – PART 2

Subject to applicable laws and regulations, in no event shall Airbus be liable for any consequential, special, indirect, incidental, punitive or exemplary damages and Airbus's liability to the State shall not exceed two times (2X) the total Contract price set forth in Contract Agreement, Section 1.8 of the *Contract Agreement –Part 1-General Provisions*.

Notwithstanding the foregoing, the limitation of liability in this SOW Section 12.2 shall not apply to Airbus's indemnification obligations set forth in the *Contract Agreement Part 1-Section 13: Indemnification* and confidentiality obligations in *Contract Agreement-Part 2- Section 11: Use of State's Information, Confidentiality*, which shall be unlimited.

12.3 State's Immunity

Notwithstanding the foregoing, nothing herein contained shall be deemed to constitute a waiver of the sovereign immunity of the State, which immunity is hereby reserved to the State. This covenant shall survive termination or Contract conclusion.

12.4 Survival

This *Contract Agreement- Part 2-Section 12: Limitation of Liability* shall survive termination or Contract conclusion.

13. TERMINATION

This Section 13 shall survive the termination or Contract Conclusion.

13.1 Termination for Default

Any one or more of the following acts or omissions of Airbus shall constitute an event of default hereunder ("Event of Default")

- a. Failure to perform the Services satisfactorily or on schedule;
- b. Failure to submit any report required; and/or
- c. Failure to perform any other covenant, term or condition of the Contract

13.1.1 Upon the occurrence of any Event of Default, the State may take any one or more, or all, of the following actions:

- a. Unless otherwise provided in the Contract, the State shall provide Airbus written notice of default and require it to be remedied within, in the absence of a greater or lesser specification of time, within thirty (30) days from the date of notice, unless otherwise indicated within by the State ("Cure Period"). If Airbus fails to cure the default within the Cure Period, the State may terminate the Contract effective two (2) days after giving Airbus notice of termination, at its sole discretion, treat the Contract as breached and pursue its remedies at law or in equity or both.
- b. Give Airbus a written notice specifying the Event of Default and suspending all payments to be made under the Contract and ordering that the portion of

Contract 2015-049 Agreement-Part 2

Initial and Date All Pages:

Airbus initials: AC

Date: 7-21-2015

**STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT – PART 2**

the Contract price which would otherwise accrue to Airbus during the period from the date of such notice until such time as the State determines that Airbus has cured the Event of Default shall never be paid to Airbus.

- c. Set off against any other obligations the State may owe to Airbus any damages the State suffers by reason of any Event of Default;
- d. Treat the Contract as breached and pursue any of its remedies at law or in equity, or both.
- e. Procure Services that are the subject of the Contract from another source and Airbus shall be liable for reimbursing the State for the replacement Services, and all administrative costs directly related to the replacement of the Contract and procuring the Services from another source, such as costs of competitive bidding, mailing, advertising, applicable fees, charges or penalties, and staff time costs; all of which shall be subject to the limitations of liability set forth in the Contract..

13.1.2 Airbus shall provide the State with written notice of default, and the State shall cure the default within thirty (30) days.

13.1.3 Notwithstanding the foregoing, nothing herein contained shall be deemed to constitute a waiver of the sovereign immunity of the State, which immunity is hereby reserved to the State. This covenant shall survive termination or Contract Conclusion.

13.2 Termination for Convenience

13.2.1 The State may, at its sole discretion, terminate the Contract for convenience, in whole or in part, by thirty (30) days written notice to Airbus. In the event of a termination for convenience, the State shall pay Airbus the agreed upon price, if separately stated in this Contract, for Deliverables for which Acceptance has been given by the State. Amounts for Services or Deliverables provided prior to the date of termination for which no separate price is stated under the Contract shall be paid, in whole or in part, generally in accordance with Contract Exhibit B, *Price and Payment Schedule*, of the Contract.

13.2.2 During the thirty (30) day period, Airbus shall wind down and cease Services as quickly and efficiently as reasonably possible, without performing unnecessary Services or activities and by minimizing negative effects on the State from such winding down and cessation of Services.

13.3 Termination for Conflict of Interest

13.3.1 The State may terminate the Contract by written notice if it determines that a conflict of interest exists, including but not limited to, a violation by any of the

Contract 2015-049 Agreement-Part 2

Initial and Date All Pages:

Airbus initials: ac

Date: 7-21-2015

Page 13 of 28

**STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT – PART 2**

parties hereto of applicable laws regarding ethics in public acquisitions and procurement and performance of Contracts.

In such case, the State shall be entitled to a pro-rated refund of any current development, support, and maintenance costs. The State shall pay all other contracted payments that would have become due and payable if Airbus did not know, or reasonably did not know, of the conflict of interest.

- 13.3.2** In the event the Contract is terminated as provided above pursuant to a violation by Airbus, the State shall be entitled to pursue the same remedies against Airbus as it could pursue in the event of a default of the Contract by Airbus.

13.4 Termination Procedure

- 13.4.1** Upon termination of the Contract, the State, in addition to any other rights provided in the Contract, may require Airbus to deliver to the State any property, including without limitation, Software and Written Deliverables, for such part of the Contract as has been terminated.

- 13.4.2** After receipt of a notice of termination, and except as otherwise directed by the State, Airbus shall:

- a. Stop work under the Contract on the date, and to the extent specified, in the notice;
- b. Promptly, but in no event longer than thirty (30) days after termination, terminate its orders and subcontracts related to the work which has been terminated and settle all outstanding liabilities and all claims arising out of such termination of orders and subcontracts, with the approval or ratification of the State to the extent required, which approval or ratification shall be final for the purpose of this Section;
- c. Take such action as the State directs, or as necessary to preserve and protect the property related to the Contract which is in the possession of Airbus and in which the State has an interest;
- d. Transfer title to the State and deliver in the manner, at the times, and to the extent directed by the State, any property which is required to be furnished to the State and which has been accepted or requested by the State; and
- e. Provide written Certification to the State that Airbus has surrendered to the State all said property.
- f. Assist in Transition Services, as reasonably requested by the State at no additional cost.

Contract 2015-049 Agreement-Part 2

Initial and Date All Pages:

Airbus initials: nc

Date: 7-21-2015

**STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT – PART 2**

14. CHANGE OF OWNERSHIP

In the event that Airbus should change ownership for any reason whatsoever, the State shall have the option of continuing under the Contract with Airbus, its successors or assigns for the full remaining term of the Contract; continuing under the Contract with Airbus, its successors or assigns for such period of time as determined necessary by the State; or immediately terminate the Contract without liability to Airbus, its successors or assigns.

15. ASSIGNMENT, DELEGATION AND SUBCONTRACTS

15.1 Airbus shall not assign, delegate, subcontract, or otherwise transfer any of its interest, rights, or duties under the Contract without the prior written consent of the State. Such consent shall not be unreasonably withheld. Any attempted transfer, assignment, delegation, or other transfer made without the State's prior written consent shall be null and void, and may constitute an event of default at the sole discretion of the State.

15.2 Airbus shall remain wholly responsible for performance of the entire Contract even if assignees, delegates, Subcontractors, or other transferees ("Assigns") are used, unless otherwise agreed to in writing by the State, and the Assigns fully assumes in writing any and all obligations and liabilities under the Contract from the Effective Date. In the absence of a written assumption of full obligations and liabilities of the Contract, any permitted assignment, delegation, subcontract, or other transfer shall neither relieve Airbus of any of its obligations under the Contract nor affect any remedies available to the State against Airbus that may arise from any event of default of the provisions of the contract. The State shall consider Airbus to be the sole point of contact with regard to all contractual matters, including payment of any and all charges resulting from the Contract.

15.3 Notwithstanding the foregoing, nothing herein shall prohibit Airbus from assigning the Contract to the successor of all or substantially all of the assets or business of Airbus provided that the successor fully assumes in writing all obligations and responsibilities under the Contract. In the event that Airbus should change ownership, as permitted under this Contract Agreement Part 2, Section 14: *Change of Ownership*, the State shall have the option to continue under the Contract with Airbus, its successors or assigns for the full remaining term of the Contract; continue under the Contract with Airbus, its successors or assigns for such period of time as determined necessary by the State; or immediately terminating the Contract without liability to Airbus, its successors or assigns.

16. DISPUTE RESOLUTION

Prior to the filing of any formal proceedings with respect to a dispute (other than an action seeking injunctive relief with respect to intellectual property rights or Confidential Information), the party believing itself aggrieved (the "Invoking Party") shall call for progressive management involvement in the dispute negotiation by written notice to the other party. Such notice shall be without prejudice to the Invoking Party's right to any other remedy permitted under the Contract.

The parties shall use reasonable efforts to arrange personal meetings and/or telephone conferences as needed, at mutually convenient times and places, between negotiators for the

Contract 2015-049 Agreement-Part 2

Initial and Date All Pages:

Airbus initials: AL

Date: 7-21-2015

**STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT - PART 2**

parties at the following successive management levels, each of which shall have a period of allotted time as specified below in which to attempt to resolve the dispute:

Contract 2015-049 Agreement-Part 2

Initial and Date All Pages:

Airbus initials: AK

Date: 7-21-2015

**STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT – PART 2**

Dispute Resolution Responsibility and Schedule Table

LEVEL	AIRBUS	STATE	CUMULATIVE ALLOTTED TIME
Primary	Hope Baker, Account Representative;	Thomas Flynn HAN Coordinator	5 Business Days
First	Kathy Richter, Inside Sales Manager;	Neil Twitchell Administrator 1	10 Business Days
Second	Mark Portanova, National Sales Manager;	Director of Public Health Services	15 Business Days
Third	Mike Pavick, Vice President, Sales and Channel Management;	Nicholas A. Toumpas DHHS Commissioner	20 Business Days

Other Services

Other services not specifically identified as being included in this Support Plan, including but not limited to training, implementation services, and custom development, are not included.

The allotted time for the first level negotiations shall begin on the date the Invoking Party's notice is received by the other party. Subsequent allotted time is days from the date that the original Invoking Party's notice is received by the other party.

17. RESERVED

18. GENERAL PROVISIONS

18.1 Travel Expenses

The State will not be responsible for any travel or out of pocket expenses incurred in the performance of the Services.

Airbus must assume all travel and related expenses by "fully loading" the proposed labor rates to include, but not limited to: meals, hotel/housing, airfare, car rentals, car mileage, and out of pocket expenses.

18.2 Shipping and Delivery Fee Exemption

The State will not pay for any shipping or delivery fees unless specifically itemized in the Contract.

18.3 Project Workspace and Office Equipment

The State agency will work with Airbus to determine the requirements for providing all necessary workspace and office equipment, including desktop computers for Airbus's staff.

Contract 2015-049 Agreement-Part 2

Initial and Date All Pages:

Airbus initials: AL

Date: 7-21-2015

**STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT – PART 2**

18.4 Access/Cooperation

As applicable, and reasonably necessary, and subject to the applicable State and federal laws and regulations and restrictions imposed by third parties upon the State, the State shall provide Airbus with access to all program files, libraries, personal computer-based systems, software packages, network systems, security systems, and hardware as required to complete contracted services.

The State shall use reasonable efforts to provide approvals, authorizations, and decisions reasonably necessary to allow Airbus to perform its obligations under the Contract.

18.5 Required Work Procedures

All work done must conform to standards and procedures established by the DoIT and the State.

18.6 Computer Use

In consideration for receiving access to and use of the computer facilities, network, licensed or developed software, software maintained or operated by any of the State entities, systems, equipment, Documentation, information, reports, or data of any kind (hereinafter "Information"), Airbus understands and agrees to the following rules:

- a. Every Authorized User has the responsibility to assure the protection of information from unauthorized access, misuse, theft, damage, destruction, modification, or disclosure.
- b. That information shall be used solely for conducting official State business, and all other use or access is strictly forbidden including, but not limited to, personal, or other private and non-State use and that at no time shall Airbus access or attempt to access any information without having the express authority to do so.
- c. That at no time shall Airbus access or attempt to access any information in a manner inconsistent with the approved policies, procedures, and /or agreements relating to system entry/access.
- d. That all software licensed, developed, or being evaluated by the State cannot be copied, shared, distributed, sub-licensed, modified, reverse engineered, rented, or sold, and that at all times Airbus must use utmost care to protect and keep such software strictly confidential in accordance with the license or any other Agreement executed by the State. Only equipment or software owned, licensed, or being evaluated by the State, can be used by Airbus. Personal software (including but not limited to palmtop sync software) shall not be installed on any equipment.
- e. That if Airbus is found to be in violation of any of the above-stated rules, the User may face removal from the State Contract, and/or criminal or civil prosecution, if the act constitutes a violation of law.

Contract 2015-049 Agreement-Part 2

Initial and Date All Pages:

Airbus initials: RL

Date: 7-21-2015

**STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT - PART 2**

18.7 Email Use

Mail and other electronic communication messaging systems are State of New Hampshire property and are to be used for business purposes only. Email is defined as "internal Email systems" or "State-funded Email systems". Airbus understands and agrees that use of email shall follow State standard policy (available upon request).

18.8 Internet/Intranet Use

The Internet/Intranet is to be used for access to and distribution of information in direct support of the business of the State of New Hampshire according to State standard policy (available upon request).

18.9 Regulatory Government Approvals

Airbus shall obtain all necessary and applicable regulatory or other governmental approvals necessary to perform its obligations under the Contract.

18.10 Force Majeure

Neither Airbus nor the State shall be responsible for delays or failures in performance resulting from events beyond the control of such party and without fault or negligence of such party. Such events shall include, but not be limited to, acts of God, strikes, lock outs, riots, and acts of War, epidemics, acts of Government, fire, power failures, nuclear accidents, earthquakes, and unusually severe weather.

Except in the event of the foregoing, Force Majeure events shall not include Airbus's inability to hire or provide personnel needed for Airbus's performance under the Contract.

18.11 Insurance

18.11.1 Airbus Insurance Requirement

See Contract Agreement Part 1-Form P-37 Section 14.

18.12 Exhibits

The Exhibits referred to, in and attached to the Contract are incorporated by reference as if fully included in the text.

18.13 Venue and Jurisdiction

Any action on the Contract may only be brought in the State of New Hampshire Merrimack County Superior Court.

18.14 Survival

The terms, conditions and warranties contained in the Contract that by their context are intended to survive the completion of the performance, cancellation or termination of the Contract shall so survive, including, but not limited to, the terms of the *Contract Agreement Exhibit D Section 3: Records Retention and Access Requirements*, *Contract Agreement Exhibit D Section 4: Accounting Requirements*, and Contract Agreement Part

**STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT – PART 2**

2-Section 11: *Use of State's Information, Confidentiality* and Contract Agreement Part 1-
Section 13: *Indemnification* which shall all survive the termination of the Contract.

18.15 Reserved

Contract 2015-049 Agreement-Part 2

Initial and Date All Pages:

Airbus initials: RC
Date: 7-21-2015

**STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT – PART 2**

TERMS AND DEFINITIONS

The following general contracting terms and definitions apply except as specifically noted elsewhere in this document.

Acceptance	Notice from the State that a Deliverable has satisfied Acceptance Test or Review.
Acceptance Letter	An Acceptance Letter provides notice from the State that a Deliverable has satisfied Acceptance Tests or Review.
Acceptance Period	The timeframe during which the Acceptance Test is performed.
Acceptance Test Plan	The Acceptance Test Plan provided by Airbus and agreed to by the State that describes at a minimum, the specific Acceptance process, criteria, and Schedule for Deliverables.
Acceptance Test and Review	Tests performed to determine that no Defects exist in the application Software or the System.
Access Control	Supports the management of permissions for logging onto a computer or network.
Agreement	A contract duly executed and legally binding.
Airbus DS Communications, Inc.	Contracted Vendor
Appendix	Supplementary material that is collected and appended at the back of a document.
Audit Trail Capture and Analysis	Supports the identification and monitoring of activities within an application or system
Auto Import	Directs the Communicator to watch a designed directory or folder for a data file, which is automatically imported without manual intervention based on a designated schedule/frequency.
Best and Final Offer (BAFO)	For negotiated procurements, a Vendor's final offer following the conclusion of discussions.
CCP	Change Control Procedures
CR	Change Request
COTS	Commercial Off-The-Shelf Software
CM	Configuration Management
Certification	Airbus's written declaration with full supporting and written Documentation (including without limitation test results as applicable) that Airbus has completed development of the Deliverable and certified its readiness for applicable Acceptance Testing or Review.
Change Control	Formal process for initiating changes to the proposed solution or process once development has begun.
Change Order	Formal documentation prepared for a proposed change in the Specifications.
Communicator! NXT	Web-based notification system used by the Division of Public Health Services to rapidly push out health alerts via telephone, fax, email and pager.

Contract 2015-049 Agreement-Part 2

Initial and Date All Pages:

Airbus initials: AS

Date: 7-21-2015

**STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT – PART 2**

Completion Date	End date for the Contract
Conference Bridget/Call Transfer	Serves as a virtual meeting place bringing individuals together by telephone. It can be set up to transfer call recipients to a conference bridge, live operator, help desk or other designated telephone line and it can also be used to transfer a call recipient into the Communicator.
Confidential Information	Information required to be kept Confidential from unauthorized disclosure <i>under the Contract</i> .
Contract	This Agreement between the State of New Hampshire and a Vendor, which creates binding obligations for each party to perform as specified in the Contract Documents.
Contract Conclusion	Refers to the conclusion of the Contract, for any reason, including but not limited to, the successful Contract completion, termination for convenience, or termination for default.
Contract Documents	Documents that comprise this Contract (See Contract Agreement, Section 1.1).
Contract Managers	The persons identified by the State and Airbus who shall be responsible for all contractual authorization and administration of the Contract. These responsibilities shall include but not be limited to processing Contract Documentation, obtaining executive approvals, tracking costs and payments, and representing the parties in all Contract administrative activities. (See Section 3: <i>Contract Management</i>).
Contracted Vendor/Vendor	Airbus DS Communications, Inc.
Conversion Test	A test to ensure that a Data conversion process correctly takes Data from a legacy system and successfully converts it to a form that can be used by the new System.
COTS	Commercial off the Shelf
Creator	A Security User in the Communicator who as the ability to view/edit personal contact information; create, view, modify and remove all groups assigned to his/her department; create, delete and modify his/her own scenarios and messages.
Cure Period	The thirty (30) day period following written notification of a default within which a contracted vendor must cure the default identified.
Custom Code	Code developed by Airbus specifically for this project for the State of New Hampshire.
Custom Software	Software developed by Airbus specifically for this project for the State of New Hampshire
Data	State's records, files, forms, Data and other documents or information, in either electronic or paper form, that will be used /converted by Airbus during the Contract Term.
DataSync	The Communicator! NXT has a full back up or Data Synchronization system supported by Airbus 2477/365. All information and data in the internally hosted server is back up daily.

Contract 2015-049 Agreement-Part 2

Initial and Date All Pages:

Airbus initials: AC

Date: 7-21-2015

**STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT – PART 2**

DBA	Database Administrator
Deficiencies/Defects	<p>A failure, deficiency or defect in a Deliverable resulting in a Deliverable, the Software, or the System, not conforming to its Specifications.</p> <p>Class A Deficiency – Software - Critical, does not allow System to operate, no work around, demands immediate action; <i>Written Documentation</i> - missing significant portions of information or unintelligible to State; <i>Non Software</i> - Services were inadequate and require re-performance of the Service.</p> <p>Class B Deficiency – Software - important, does not stop operation and/or there is a work around and user can perform tasks; <i>Written Documentation</i> - portions of information are missing but not enough to make the document unintelligible; <i>Non Software</i> - Services were deficient, require reworking, but do not require re-performance of the Service.</p> <p>Class C Deficiency – Software - minimal, cosmetic in nature, minimal effect on System, low priority and/or user can use System; <i>Written Documentation</i> - minimal changes required and of minor editing nature; <i>Non Software</i> - Services require only minor reworking and do not require re-performance of the Service.</p>
Deliverable	A Deliverable is any Written, Software, or Non-Software Deliverable (letter, report, manual, book, other), provided by Airbus to the State or under the terms of a Contract requirement.
Department	An agency of the State
Department of Information Technology (DoIT)	The Department of Information Technology established under RSA 21-R by the Legislature effective September 5, 2008.
DHHS	Department of Health and Human Services
Documentation	All information that describes the installation, operation, and use of the Software, either in printed or electronic format.
Digital Signature	Guarantees the unaltered state of a file
Effective Date	The Contract and all obligations of the parties hereunder shall become effective on the date the Governor and the Executive Council of the State of New Hampshire approves the Contract
Encryption	Supports the transformation of data for security purposes
Enhancements	Updates, additions, modifications to, and new releases for the Software, and all changes to the Documentation as a result of Enhancements, including, but not limited to, Enhancements produced by Change Orders.
Firm Fixed Price Contract	A Firm-Fixed-Price Contract provides a price that is not subject to increase, i.e., adjustment on the basis of Airbus's cost experience in performing the Contract.
Fully Loaded	Rates are inclusive of all allowable expenses, including, but not

Contract 2015-049 Agreement-Part 2

Initial and Date All Pages:

Airbus initials: AS

Date: 7-21-2015

**STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT – PART 2**

	limited to: meals, hotel/housing, airfare, car rentals, car mileage, and out of pocket expenses.
GAAP	Generally Accepted Accounting Principles
Governor and Executive Council	The New Hampshire Governor and Executive Council.
Identification and Authentication	Supports obtaining information about those parties attempting to log on to a system or application for security purposes and the validation of those users.
Implementation	The process for making the System fully operational for processing the Data.
Implementation Plan	Sets forth the transition from development of the System to full operation, and includes without limitation, training, business and technical procedures.
Inbound Bulletin Board	Used to deliver status updates or general information to incoming callers in the Communicator. It can be used to provide emergency or routine information.
Information Technology (IT)	Refers to the tools and processes used for the gathering, storing, manipulating, transmitting, sharing, and sensing of information including, but not limited to, Data processing, computing, information systems, telecommunications, and various audio and video technologies.
Input Validation	Ensure that the values entered by users or provided by other applications meets the size, type and format expected. Protecting the application from cross site scripting, SQL injection, buffer overflow, etc.
Intrusion Detection	Supports the detection of illegal entrance into a computer system.
Invoking Party	In a dispute, the party believing itself aggrieved.
Key Project Staff	Personnel identified by the State and by Airbus as essential to work on the Project.
Licensee	The State of New Hampshire
Non Exclusive Contract	A contract executed by the State that does not restrict the State from seeking alternative sources for the Deliverables or Services provided under the Contract.
Non-Software Deliverables	Deliverables that are not Software Deliverables or Written Deliverables, e.g., meetings, help support, services, other.
Normal Business Hours	Normal Business Hours – 8:00 a.m. to 5:00 p.m. EST, Monday through Friday excluding State of New Hampshire holidays. State holidays are: New Year's Day, Martin Luther King Day, President's Day, Memorial Day, July 4 th , Labor Day, Veterans Day, Thanksgiving Day, the day after Thanksgiving Day, and Christmas Day. Specific dates will be provided.
Not to Exceed (NTE)	An estimate of the cost of a project that a potential contractor gives to the firm negotiating a contract. An NTE includes additional funds that might be needed in case something goes wrong. It is important to note than an NTE assumes that the scope of the project does not change; it may be revised if this occurs.

Contract 2015-049 Agreement-Part 2

Initial and Date All Pages:

Airbus initials: RC

Date: 7-21-2015

**STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT – PART 2**

Notice to Proceed (NTP)	The State Contract Manager's written direction to Airbus to begin work on the Contract on a given date and time.
NXT Call Blast	Provides simultaneous message broadcast to all selected devices.
Open Data Formats	A data format based on an underlying Open Standard.
Open Source Software	Software that guarantees the user unrestricted use of the Software as defined in RSA 21-R:10 and RSA 21-R:11.
Open Standards	Specifications for the encoding and transfer of computer data that is defined in RSA 21-R:10 and RSA 21-R:13.
Operating System	System is fully functional, all Data has been loaded into the System, is available for use by the State in its daily operations.
Operational	Operational means that the System is operating and fully functional, all Data has been loaded; the System is available for use by the State in its daily operations, and the State has issued an Acceptance Letter.
Order of Precedence	The order in which Contract/Documents control in the event of a conflict or ambiguity. A term or condition in a document controls over a conflicting or ambiguous term or condition in a document that is lower in the Order of Precedence.
Project	The planned undertaking regarding the entire subject matter of a Contract and the activities of the parties related hereto.
Project Team	The group of State employees and Airbus's personnel responsible for managing the processes and mechanisms required such that the Services are procured in accordance with the Work Plan on time, on budget and to the required specifications and quality.
Project Management Plan	A document that describes the processes and methodology to be employed by Airbus to ensure a successful Project.
Project Managers	The persons identified who shall function as the State's and Airbus's representative with regard to Review and Acceptance of Contract Deliverables, invoice sign off, and review and approval of Change Requests (CR) utilizing the Change Control Procedures (CCP).
Project Staff	State personnel assigned to work with Airbus on the Project.
Proposal	The submission from a Vendor in response to the Request for a Proposal or Statement of Work.
Regression Test Plan	A plan integrated into the Work Plan used to ascertain whether fixes to Defects have caused errors elsewhere in the application/process.
Review	The process of reviewing Deliverables for Acceptance.
Review Period	The period set for review of a Deliverable. If none is specified then the Review Period is five (5) business days.
Role/Privilege Management	Supports the granting of abilities to users or groups of users of a computer, application or network.
Roster User	A Security User in the Communicator who as the ability to view and/or edit personal contact information.

Contract 2015-049 Agreement-Part 2

Initial and Date All Pages:

Airbus initials: AC

Date: 7-21-2015

**STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT – PART 2**

SaaS- Software as a Service	Occurs where the COTS application is hosted but the State does not own the license or the code. Airbus allows the use of the software as a part of their service.
Scenario	A saved set of defined parameters used to send messages to specific devices (email, phone, fax, alpha or numeric pagers) that are used by individuals in the Communicator.
Schedule	The dates described in the Work Plan for deadlines for performance of Services and other Project events and activities under the Contract
Security User	A predefined role of an individual who uses the Communicator with permissions to different features and functions of the System.
Service Level Agreement (SLA)	A signed agreement between Airbus and the State specifying the level of Service that is expected of, and provided by, Airbus during the term of the Contract.
Services	The work or labor to be performed by Airbus on the Project as described in the Contract.
Short Message Service (SMS)	Text messaging service component of phone, Web, or mobile communication systems that uses standardized communications protocols to allow fixed line or mobile phone devices to exchange short text messages.
Software	All custom Software and COTS Software provided by Airbus under the Contract.
Software Deliverables	COTS Software and Enhancements
Software License	Licenses provided to the State under this Contract.
Solution	The Solution consists of the total Solution, which includes, without limitation, Software and Services, addressing the requirements and terms of the Specifications. The off-the-shelf Software and configured Software customized for the State provided by Airbus in response to this RFP.
Specifications	The written Specifications that set forth the requirements which include, without limitation, the Contract, any performance standards, Documentation, applicable State and federal policies, laws and regulations, State technical standards, subsequent State-approved Deliverables, and other Specifications and requirements described in the Contract Documents. The Specifications are, by this reference, made a part of the Contract as though completely set forth herein.
State	STATE is defined as: State of New Hampshire Department of Health and Human Services The Division of Public Health Services 29 Hazen Drive Concord, NH 03301 Reference to the term "State" shall include applicable agencies.
Statement of Work (SOW)	A Statement of Work clearly defines the basic requirements and objectives of a Project. The Statement of Work also defines a high

Contract 2015-049 Agreement-Part 2

Initial and Date All Pages:

Airbus initials: AC

Date: 7-21-2015

**STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT - PART 2**

	level view of the architecture, performance and design requirements, the roles and responsibilities of the State and Airbus. The Contract Agreement SOW defines the results that Airbus remains responsible and accountable for achieving.
State's Confidential Records	State's information regardless of its form that is not subject to public disclosure under applicable state and federal laws and regulations, including but not limited to <u>RSA Chapter 91-A</u>
State Data	Any information contained within State systems in electronic or paper format.
State Fiscal Year (SFY)	The New Hampshire State Fiscal Year extends from July 1 st through June 30 th of the following calendar year.
State Project Leader	State's representative with regard to Project oversight.
State's Project Manager (PM)	State's representative with regard to Project management and technical matters. Agency Project Managers are responsible for review and Acceptance of specific Contract Deliverables, invoice sign off, and Review and approval of a Change Proposal (CP).
Subcontractor	A person, partnership, or company not in the employment of, or owned by, Airbus, which is performing Services under this Contract under a separate Contract with or on behalf of Airbus
System	All Software, specified hardware, and interfaces and extensions, integrated and functioning together in accordance with the Specifications.
System Administrator	A Security User in the Communicator who as the ability to: view/add, delete and/or edit all contact information; create, view, modify and remove all groups, messages and scenarios; assign security roles and password rules; reset passwords for all users.
TBD	To Be Determined
Technical Authorization	Direction to a Vendor, which fills in details, clarifies, interprets, or specifies technical requirements. It must be: (1) consistent with Statement of Work within statement of Services; (2) not constitute a new assignment; and (3) not change the terms, documents of specifications of the Contract Agreement.
Test Plan	A plan, integrated in the Work Plan, to verify the code (new or changed) works to fulfill the requirements of the Project. It may consist of a timeline, a series of tests and test data, test scripts and reports for the test results as well as a tracking mechanism.
Term	Period of the Contract from the Effective Date through termination.
Transition Services	Services and support provided when Airbus is supporting System changes.
UAT	User Acceptance Test
Unit Test	Developers create their own test data and test scenarios to verify the code they have created or changed functions properly as defined.
User	A Security User in the Communicator who has the ability to view/edit personal contact information; view, modify and remove groups assigned to his/her department; view, modify, remove,

Contract 2015-049 Agreement-Part 2

Initial and Date All Pages:

Airbus initials: hc

Date: 7-21-2015

**STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT – PART 2**

	activate and stop scenarios assigned to his/her department.
User Acceptance Testing	Tests done by knowledgeable business users who are familiar with the scope of the Project. They create/develop test cases to confirm the System was developed according to specific user requirements. The test cases and scripts/scenarios should be mapped to business requirements outlined in the user requirements documents.
User Management	Supports the administration of computer, application and network accounts within an organization
Vendor/ Contracted Vendor	Airbus whose proposal or quote was awarded the Contract with the State and who is responsible for the Services and Deliverables of the Contract.
Verification	Supports the confirmation of authority to enter a computer system, application or network.
Walk Through	A step-by-step review of a Specification, usability features or design before it is handed off to the technical team for development
Warranty Period	A period of coverage during which Airbus is responsible for providing a guarantee for products and Services delivered as defined in the Contract.
Warranty Releases	Code releases that are done during the Warranty Period.
Warranty Services	The Services to be provided by Airbus during the Warranty Period.
Work Hours	Airbus personnel shall work normal business hours between 8:00 am and 5:00 pm, eight (8) hour days, forty (40) hour weeks, excluding State of New Hampshire holidays. Changes to this schedule may be made upon agreement with the State Project Manager.
Work Plan	The overall plan of activities for the Project created in accordance with the Contract. The plan and delineation of tasks, activities and events to be performed and Deliverables to be produced under the Project as specified in Appendix C. The Work Plan shall include a detailed description of the Schedule, tasks/activities, Deliverables, critical events, task dependencies, and the resources that would lead and/or participate on each task.
Written Deliverables	Non-Software written deliverable Documentation (letter, report, manual, book, other) provided by Airbus either in paper or electronic format.
XML API	Extensible Markup Language (XML) Application Programming Interface (API) allows the Communicator to integrate with other technologies.

Contract 2015-049 Agreement-Part 2

Initial and Date All Pages:

Airbus initials: AC

Date: 7-21-2015

Page 28 of 28

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR NXT HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT - PART 3
EXHIBIT A
CONTRACT DELIVERABLES

1. DELIVERABLES, MILESTONES AND ACTIVITIES

The Communicator is a web-based high-speed notification System used by the Department of Health and Human Services (DHHS) and other internal and external partners. The System is used to communicate with appropriate persons in the event of a health alert or advisory. System capabilities include: a database of individuals, groups and scenarios. Notifications are delivered simultaneously via multiple communications devices including: telephone, cellular phone, SMS devices, satellite phones, overhead pagers, alpha and digital pager, e-mail and fax. The System is capable of running multiple scenarios or alerts simultaneously which can be activated using a computer or remotely by phone. The System allows real time monitoring of activated scenarios, reporting of activated scenarios, and the ability to fax blast. The web interface allows individuals to access the system and maintain their contact information.

The NH Health Alert Network (NH HAN) links the State DHHS to organizations critical for preparedness and response in NH: community first-responders, hospital and private laboratories, the two city health departments, CDC, and other federal agencies. The NH HAN uses the Communicator to maintain a high-speed, continuous, secure connection to the internet and provide early warning, such as broadcast email, fax, or automated (recorded message) phone call, to alert hospitals and local, state and federal authorities and the media about urgent health threats and necessary prevention and response actions.

The purpose of the NH HAN is to provide a comprehensive 24/7/365 System for public health emergency communication to a network of individuals involved in the creation, communication and response to public health emergencies. The System links all healthcare systems that participate in the Hospital Preparedness Program as well as those that are deemed necessary by the State of NH for both state and local jurisdiction health and medical response operations including local health departments, health officers, New Hampshire Public Health Laboratories, Medical Reserve Corps, and the Metropolitan Medical Response System. The System has the ability to exchange voice and/or data with all partners on demand, in real-time, when needed, and as authorized by the NH State Epidemiologist.

Airbus DS Communications, Inc. (Airbus) shall provide the State with the Communicator 4.4.2, which will meet and perform in accordance with the Specifications and Deliverables within this contract.

Prior to the commencement of work, Airbus shall provide to the State a Work Plan for review and approval by the State.

The Deliverables are set forth in the Schedule described below in Section 2. By unconditionally accepting a Deliverable, the State reserves the right to reject any and all Deliverables in the event the State detects any Deficiency in the System, in whole or in part, through completion of all Acceptance Testing, including but not limited to, Software/System Acceptance Testing, and any extensions thereof.

Pricing for Deliverables set forth in Exhibit B: *Price and Payment Schedule*. Pricing will be effective for the Term of this Contract, and any extensions thereof.

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR NXT HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT - PART 3
EXHIBIT A
CONTRACT DELIVERABLES

2. DELIVERABLES, MILESTONES, AND ACTIVITIES SCHEDULE

2.1 Implementation Schedule – Activities / Deliverables / Milestones

Reference Number	Activity, Deliverable, or Milestone	Deliverable Type	Projected Delivery Date
Project Management			
1	Kickoff Meeting Call	Non-Software	5 days after contract approval
2	Finalized Work Plan	Written	5 days after contract approval
3	Phase I Planning Meeting: <ul style="list-style-type: none"> Identify tasks Identify staff Identify core modules <ul style="list-style-type: none"> Auto Import Custom Reports Web Check In Identify add-on modules <ul style="list-style-type: none"> NXT Call Blast @ \$2,500 In-Bound Bulletin Board cost included EFax @ \$7,350/year XML API cost included Transfer to Conference Bridge @ \$2,500 Weekly status meeting with weekly status reports 	Non-Software and Written	5 days after contract approval
Project Implementation			
4	Phase II Implementation: <ul style="list-style-type: none"> Set up software at hosted site for update including the Inbound Bulletin Board and XML API at no additional cost First year charge of \$1,500 for standard implementation processes NXT Call Blast @ \$2,500/year EFax @ \$7,350/year 	Software and Written	15 days after contract approval

Contract 2015-049 Agreement – Part 3 Exhibit A: Contract Deliverables

Initial and Date All Pages:

Airbus Initials RL

Date: 7-21-15

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR NXT HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT - PART 3
EXHIBIT A
CONTRACT DELIVERABLES

Reference Number	Activity, Deliverable, or Milestone	Deliverable Type	Projected Delivery Date
	<ul style="list-style-type: none"> Conference Bridge @ \$2,500/year User acceptance training User acceptance testing and acceptance Weekly status meeting with weekly status reports 		
5	Phase III Cut Over: <ul style="list-style-type: none"> Confirmed site ready Acceptance testing State accepts the System Parallel operation between the in-house and hosted Systems for a period of time (6 weeks) Final load of production data to new System Flash cut to hosted System Verify that redundant System is ready (use in place of primary System for assurance) Notify DoIT that in house System is no longer under vendor support and maintenance Weekly status meeting with weekly status reports 	Software, Non-Software and Written	20 days after contract approval
6	Project Close Out Meeting	Non-Software	10 weeks after contract approval
Licensing, Hosting Maintenance and Support: Year 1			
7	Phase IV Post cut over support <ul style="list-style-type: none"> Final System Acceptance License Fee (Includes Hosting Maintenance and Support for 9,000 contacts): Year 1	Non-Software and Written	9 weeks after contract approval
Training			
8	Training – Annual Web-Based (up to 10 seats included in the annual cost)	Non-Software	10/1/15
Licensing, Hosting Maintenance and Support, Add-On Modules, and Training: Year 2			
9	License Fee (Includes Hosting Maintenance and Support for 9,000 contacts): Year 2	Software & Non-Software	10/1/16
10	<ul style="list-style-type: none"> Conference Bridge @ \$2,500/year: Year 2 	Software	

Contract 2015-049 Agreement – Part 3 Exhibit A: Contract Deliverables

Initial and Date All Pages:

Airbus Initials nc

Date: 7-21-2015

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR NXT HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT - PART 3
EXHIBIT A
CONTRACT DELIVERABLES

Reference Number	Activity, Deliverable, or Milestone	Deliverable Type	Projected Delivery Date
	<ul style="list-style-type: none"> Efax @ \$7,350/year: Year 2 NXT Call Blast @ \$2,500/year: Year 2 		
11	Training on-site for 5 participants (3 days): Year 2	Non-Software	
Licensing, Hosting Maintenance and Support, Add-On Modules, and Training: Year 3			
12	License Fee (Includes Hosting Maintenance and Support for 9,000 contacts): Year 3	Software & Non-Software	10/1/17
13	<ul style="list-style-type: none"> Conference Bridge @ \$2,500/year: Year 3 Efax @ \$7,350/year: Year 3 NXT Call Blast @ \$2,500/year: Year 3 	Software	
14	Web-Based Training for up to 10 participants (in addition to the one free session per year): Year 3	Non-Software	
Licensing, Hosting Maintenance and Support, Add-On Modules, and Training: Year 4			
15	License Fee (Includes Hosting Maintenance and Support for 9,000 contacts): Year 4	Software & Non-Software	10/1/18
16	<ul style="list-style-type: none"> Conference Bridge @ \$2,500/year: Year 4 Efax @ \$7,350/year: Year 4 NXT Call Blast @ \$2,500/year: Year 4 	Software	
17	Web-Based Training for up to 10 participants (in addition to the one free session per year): Year 4	Non-Software	
Licensing, Hosting Maintenance and Support, Add-On Modules, and Training: Year 5			
18	License Fee (Includes Hosting Maintenance and Support for 9,000 contacts): Year 5	Software & Non-Software	10/1/19
19	<ul style="list-style-type: none"> Conference Bridge @ \$2,500/year: Year 5 Efax @ \$7,350/year: Year 5 NXT Call Blast @ \$2,500/year: Year 5 	Software	

Contract 2015-049 Agreement – Part 3 Exhibit A: Contract Deliverables

Initial and Date All Pages:

Airbus Initials RL

Date: 7-21-2015

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR NXT HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT - PART 3
EXHIBIT A
CONTRACT DELIVERABLES

Reference Number	Activity, Deliverable, or Milestone	Deliverable Type	Projected Delivery Date
20	Web-Based Training for up to 10 participants (in addition to the one free session per year): Year 5	Non-Software	

Contract 2015-049 Agreement – Part 3 Exhibit A: Contract Deliverables

Initial and Date All Pages:

Airbus Initials RL

Date: 7-21-2015

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR NXT HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT - PART 3
EXHIBIT B
PRICE AND PAYMENT SCHEDULE

1. DELIVERABLE PAYMENT SCHEDULE

1.1 Not to Exceed Price

This is a Not to Exceed Price (NTE) Contract for Software as a Service (SaaS) totaling \$198,950 for the period between the Effective Date of Governor and Executive Council approval through August 31, 2020, Airbus shall be responsible for performing its obligations in accordance with the Contract. This Contract will allow Airbus to invoice the State for the following activities, Deliverables, or milestones at NTE rates appearing in the price and payment tables below:

Table 1.1.1 – Deliverable Payment Schedule

Deliverable Payment Schedule					
Reference Number	Activity, Deliverable, or Milestone	Deliverable Type	Projected Delivery Date	Price	Payment Amount
Project Management					
1	Kickoff Meeting Call	Non-Software	10 days after contract approval		
2	Finalized Work Plan	Written	10 days after contract approval		
3	Phase I Planning Meeting: <ul style="list-style-type: none"> Identify tasks Identify staff Identify core modules <ul style="list-style-type: none"> Call Blast XML API Identify add-on modules <ul style="list-style-type: none"> Conference Bridge EFax In-Bound Bulletin Board Weekly status meetings with weekly status reports 	Non-Software and Written	10 days after contract approval		
Project Implementation					
4	Phase II Implementation: <ul style="list-style-type: none"> Set up software at hosted site includes Inbound 	Software and Written	15 days after contract approval	\$12,350	\$12,350

Contract 2015-049 Agreement – Part 3 Exhibit B-Price and Payment Schedule

Initial and Date All Pages:

Airbus Initials RC

Date: 7-21-2015

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR NXT HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT - PART 3
EXHIBIT B
PRICE AND PAYMENT SCHEDULE

Deliverable Payment Schedule					
Reference Number	Activity, Deliverable, or Milestone	Deliverable Type	Projected Delivery Date	Price	Payment Amount
	<ul style="list-style-type: none"> Bulletin Board and XML API • Conference Bridge @ \$2,500/year • Efax @ \$7,350/year • NXT Call Blast @ \$2,500/year • User acceptance training • User acceptance testing and acceptance • Weekly status meeting with weekly status reports 				
5	Phase III Cut Over: <ul style="list-style-type: none"> • Confirmed site ready • Acceptance testing • State accepts the System • Parallel operation between the in-house and hosted Systems for a period of time (6 weeks) • Final load of production data to new System • Flash cut to hosted System • Verify that redundant System is ready (use in place of primary System for assurance) • Notify DoIT that in house System is no longer under vendor support and maintenance • Weekly status meeting with weekly status reports 	Non-Software, Software and Written	20 days after contract approval		

Contract 2015-049 Agreement – Part 3 Exhibit B-Price and Payment Schedule

Initial and Date All Pages:

Airbus Initials AC

Date: 7-21-2015

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR NXT HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT - PART 3
EXHIBIT B
PRICE AND PAYMENT SCHEDULE

Deliverable Payment Schedule					
Reference Number	Activity, Deliverable, or Milestone	Deliverable Type	Projected Delivery Date	Price	Payment Amount
6	Project Close Out Meeting	Non-Software	10 weeks after contract approval		
Licensing, Hosting Maintenance and Support: Year 1					
7	Phase IV Post cut over support <ul style="list-style-type: none"> Final System Acceptance License Fee Includes Hosting Maintenance and Support for 9,000 contacts @ \$21,787: Year 1 Includes a first-year charge of \$1,500 for standard implementation processes: Year 1 	Non-Software and Written	9 weeks after contract approval	\$27,500	\$27,500
Training					
8	Training – Annual Web-Based (up to 10 seats included in the annual cost)	Non-Software	10/1/15	Included	
	Subtotal Implementation, Add-On Modules, Training and First Year Hosting			\$39,850	\$39,850
Licensing, Hosting Maintenance and Support, Add-On Modules, and Training: Year 2					
9	License Fee (Includes Hosting Maintenance and Support for 9,000 contacts): Year 2	Software & Non-Software	10/1/16	\$26,000	\$26,000
10	<ul style="list-style-type: none"> Conference Bridge @ \$2,500/year: Year 2 Efax @ \$7,350/year: Year 2 NXT Call Blast @ \$2,500/year: Year 2 	Software		\$12,350	\$12,350
11	Training on-site for 5 participants (2 days): Year 2	Non-Software		\$4,200	\$4,200

Contract 2015-049 Agreement – Part 3 Exhibit B-Price and Payment Schedule

Initial and Date All Pages:

Airbus Initials RC

Date: 7-21-2015

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR NXT HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT - PART 3
EXHIBIT B
PRICE AND PAYMENT SCHEDULE

Deliverable Payment Schedule					
Reference Number	Activity, Deliverable, or Milestone	Deliverable Type	Projected Delivery Date	Price	Payment Amount
Licensing, Hosting Maintenance and Support, Add-On Modules, and Training: Year 3					
12	License Fee (Includes Hosting Maintenance and Support for 9,000 contacts): Year 3	Software & Non-Software	10/1/17	\$26,000	\$26,000
13	<ul style="list-style-type: none"> Conference Bridge @ \$2,500/year: Year 3 Efax @ \$7,350/year: Year 3 NXT Call Blast @ \$2,500/year: Year 3 	Software		\$12,350	\$12,350
14	Web-Based Training for up to 10 participants (in addition to the one free session per year): Year 3	Non-Software		\$500	\$500
Licensing, Hosting Maintenance and Support, Add-On Modules, and Training: Year 4					
15	License Fee (Includes Hosting Maintenance and Support for 9,000 contacts): Year 4	Software & Non-Software	10/1/18	\$26,000	\$26,000
16	<ul style="list-style-type: none"> Conference Bridge @ \$2,500/year: Year 4 Efax @ \$7,350/year: Year 4 NXT Call Blast @ \$2,500/year: Year 4 	Software		\$12,350	\$12,350
17	Web-Based Training for up to 10 participants (in addition to the one free session per year): Year 4	Non-Software		\$500	\$500
Licensing, Hosting Maintenance and Support, Add-On Modules, and Training: Year 5					
18	License Fee (Includes Hosting Maintenance and Support for 9,000 contacts): Year 5	Software & Non-Software	10/1/19	\$26,000	\$26,000

Contract 2015-049 Agreement – Part 3 Exhibit B-Price and Payment Schedule

Initial and Date All Pages:

Airbus Initials AC

Date: 7-21-2015

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR NXT HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT - PART 3
EXHIBIT B
PRICE AND PAYMENT SCHEDULE

Deliverable Payment Schedule					
Reference Number	Activity, Deliverable, or Milestone	Deliverable Type	Projected Delivery Date	Price	Payment Amount
19	<ul style="list-style-type: none"> Conference Bridge @ \$2,500/year: Year 5 Efax @ \$7,350/year: Year 5 NXT Call Blast @ \$2,500/year: Year 5 	Software		\$12,350	\$12,350
20	Web-Based Training for up to 10 participants (in addition to the one free session per year): Year 5	Non-Software		\$500	\$500
	Subtotal Ongoing Hosting Maintenance and Support, Add-On Modules, Training: Year 2-5			\$159,100	\$159,100
	Not to Exceed Total			\$198,950	\$198,950

Table 1.1.2 – Detailed License Deliverables and Pricing

Detailed License Deliverables and Pricing			
Description	License Type	Quantity	Net Price-License
SaaS			
License (Includes Hosting Maintenance and Support for 9,000 contacts)	non-exclusive, non-transferable, worldwide term	1	\$26,000
First-year Implementation Processes (one-time charge)		1	\$1,500
Application Products			
XML API		1	Included
In-Bound Bulletin Board		1	Included
EFax		1	\$7,350
NXT Call Blast		1	\$2,500
Conference Bridge		1	\$2,500
Grand Total			\$39,850

Contract 2015-049 Agreement – Part 3 Exhibit B-Price and Payment Schedule

Initial and Date All Pages:

Airbus Initials AC

Date: 7-21-15

**STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR NXT HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT - PART 3
EXHIBIT B
PRICE AND PAYMENT SCHEDULE**

Table 1.1.3 - Airbus SaaS Pricing Worksheet

Airbus SaaS Pricing Worksheet					
SaaS	10/1/2015- 8/31/2016	10/1/2016- 8/31/2017	10/1/2017- 8/31/2018	10/1/2018- 8/31/2019	10/1/2019- 8/31/2020
License (Includes Hosting Maintenance and Support for 9,000 contacts)	\$26,000	\$26,000	\$26,000	\$26,000	\$26,000
Implementation Processes (one-time charge)	\$1,500	\$0.00	\$0.00	\$0.00	\$0.00
Onsite training for 5 participants	\$0.00	\$4,200	\$0.00	\$0.00	\$0.00
Additional Annual Web- Training	\$0.00	\$0.00	\$500	\$500	\$500
Application Products					
XML API	Included	Included	Included	Included	Included
In-Bound Bulletin Board	Included	Included	Included	Included	Included
EFax	\$7,350	\$7,350	\$7,350	\$7,350	\$7,350
NXT Call Blast	\$2,500	\$2,500	\$2,500	\$2,500	\$2,500
Conference Bridge	\$2,500	\$2,500	\$2,500	\$2,500	\$2,500

2. TOTAL CONTRACT PRICE

Notwithstanding any provision in the Contract to the contrary, and notwithstanding unexpected circumstances, in no event shall the total of all payments made by the State exceed \$198,950.

The State will not be responsible for any travel or out of pocket expenses incurred in the performance of the Services performed under this Contract.

3. INVOICING

Airbus shall submit correct invoices to the State for all amounts to be paid by the State. All invoices submitted shall be subject to the State's prior written approval, which shall not be unreasonably withheld. Airbus shall only submit invoices for Services or Deliverables as permitted by the Contract. Invoices must be in a format as determined by the State and contain detailed information, including without limitation: itemization of each Deliverable and identification of the Deliverable for which payment is

**STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR NXT HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT - PART 3
EXHIBIT B
PRICE AND PAYMENT SCHEDULE**

sought, and the Acceptance date triggering such payment; date of delivery and/or installation; monthly maintenance charges; any other Project costs or retention amounts if applicable.

Upon Acceptance of a Deliverable, and a properly documented and undisputed invoice, the State will pay the correct and undisputed invoice within thirty (30) days of invoice receipt. Invoices will not be backdated and shall be promptly dispatched.

Invoices shall be sent to:

Shelley Swanson
Department of Health and Human Services
Division of Public Health Services
Bureau of Infectious Disease Control
29 Hazen Drive
Concord, NH 03301

4. PAYMENT ADDRESS

All payments shall be sent to the following address:
Airbus DS Communications, Inc.
117 Seaboard Lane, Suite D-100
Franklin, TN 37067

5. OVERPAYMENTS TO AIRBUS

Airbus shall promptly, but no later than fifteen (15) business days, return to the State the full amount of any overpayment or erroneous payment upon discovery or notice from the State.

6. CREDITS

The State may apply credits due to the State arising out of this Contract, against Airbus' invoices with appropriate information attached.

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR NXT HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT - PART 3
EXHIBIT C
SPECIAL PROVISIONS

1. SPECIAL PROVISIONS

Contractor's Obligations: The Contractor covenants and agrees that all funds received by the Contractor under the Contract shall be used only as payment to the Contractor for services provided to eligible individuals and, in the furtherance of the aforesaid covenants, the Contractor hereby covenants and agrees as follows:

- 1.1 Gratuities or Kickbacks:** The Contractor agrees that it is a breach of this Contract to accept or make a payment, gratuity or offer of employment on behalf of the Contractor, any Sub-Contractor or the State in order to influence the performance of the Scope of Work detailed in Exhibit A of this Contract. The State may terminate this Contract and any sub-contract or sub-agreement if it is determined that payments, gratuities or offers of employment of any kind were offered or received by any officials, officers, employees or agents of the Contractor or Sub-Contractor.
- 1.2 Retroactive Payments:** Notwithstanding anything to the contrary contained in the Contract or in any other document, contract or understanding, it is expressly understood and agreed by the parties hereto, that no payments will be made hereunder to reimburse the Contractor for costs incurred for any purpose or for any services provided to any individual prior to the Effective Date of the Contract and no payments shall be made for expenses incurred by the Contractor for any services provided prior to the date on which the individual applies for services or (except as otherwise provided by the federal regulations) prior to a determination that the individual is eligible for such services.
- 1.3 Conditions of Purchase:** Notwithstanding anything to the contrary contained in the Contract, nothing herein contained shall be deemed to obligate or require the Department to purchase services hereunder at a rate which reimburses the Contractor in excess of the Contractor's costs, at a rate which exceeds the amounts reasonable and necessary to assure the quality of such service, or at a rate which exceeds the rate charged by the Contractor to ineligible individuals or other third party funders for such service. If at any time during the term of this Contract or after receipt of the Final Expenditure Report hereunder, the Department shall determine that the Contractor has used payments hereunder to reimburse items of expense other than such costs, or has received payment in excess of such costs or in excess of such rates charged by the Contractor to ineligible individuals or other third party funders, the Department may elect to:
 - 1.3.1. Renegotiate the rates for payment hereunder, in which event new rates shall be established;
 - 1.3.2. Deduct from any future payment to the Contractor the amount of any prior reimbursement in excess of costs;
 - 1.3.3. Demand repayment of the excess payment by the Contractor in which event failure to make such repayment shall constitute an Event of Default hereunder. When the Contractor is permitted to determine the eligibility of individuals for services, the Contractor agrees to reimburse the Department for all funds paid by the Department to the Contractor for services provided to any individual who is found by the Department to be ineligible for such services at any time during the period of retention of records established herein.

**STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR NXT HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT - PART 3
EXHIBIT C
SPECIAL PROVISIONS**

- 1.4 Maintenance of Records:** In addition to the eligibility records specified above, the Contractor covenants and agrees to maintain the following records during the Contract Period:
- 1.4.1 **Fiscal Records:** books, records, documents and other data evidencing and reflecting all costs and other expenses incurred by the Contractor in the performance of the Contract, and all income received or collected by the Contractor during the Contract Period, said records to be maintained in accordance with accounting procedures and practices which sufficiently and properly reflect all such costs and expenses, and which are acceptable to the Department, and to include, without limitation, all ledgers, books, records, and original evidence of costs such as purchase requisitions and orders, vouchers, requisitions for materials, inventories, valuations of in-kind contributions, labor time cards, payrolls, and other records requested or required by the Department.
- 1.4.2 **Statistical Records:** Statistical, enrollment, attendance or visit records for each recipient of services during the Contract Period, which records shall include all records of application and eligibility (including all forms required to determine eligibility for each such recipient), records regarding the provision of services and all invoices submitted to the Department to obtain payment for such services.
- 4.3. **Medical Records:** Where appropriate and as prescribed by the Department regulations, the Contractor shall retain medical records on each patient/recipient of services.
- 1.5 Confidentiality of Records:** All information, reports, and records maintained hereunder or collected in connection with the performance of the services and the Contract shall be Confidential and shall not be disclosed by the Contractor, provided however, that pursuant to state laws and the regulations of the Department regarding the use and disclosure of such information, disclosure may be made to public officials requiring such information in connection with their official duties and for purposes directly connected to the administration of the services and the Contract; and provided further, that the use or disclosure by any party of any information concerning a recipient for any purpose not directly connected with the administration of the Department or the Contractor's responsibilities with respect to purchased services hereunder is prohibited except on written consent of the recipient, his attorney or guardian.
- Notwithstanding anything to the contrary contained herein the covenants and conditions contained in the Paragraph shall survive the termination of the Contract for any reason whatsoever.
- 1.6 Completion of Services:** Disallowance of Costs: Upon the purchase by the Department of the maximum number of units provided for in the Contract and upon payment of the price limitation hereunder, the Contract and all the obligations of the parties hereunder (except such obligations as, by the terms of the Contract are to be performed after the end of the term of this Contract and/or survive the termination of the Contract) shall terminate, provided however, that if, upon review of the Final Expenditure Report the Department shall disallow any expenses claimed by the Contractor as costs hereunder the Department shall retain the right, at its discretion, to deduct the amount of such expenses as are disallowed or to recover such sums from the Contractor.
- 1.7 Credits:** All documents, notices, press releases, research reports and other materials prepared during or resulting from the performance of the services of the Contract shall include the following statement:

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR NXT HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT - PART 3
EXHIBIT C
SPECIAL PROVISIONS

1.7.1 The preparation of this (report, document etc.) was financed under a Contract with the State of New Hampshire, DHHS, with funds provided in part by the State of New Hampshire and/or such other funding sources as were available or required, e.g., the United States Department of Health and Human Services.

- 1.8 Prior Approval and Copyright Ownership:** All materials (written, video, audio) produced or purchased under the contract shall have prior approval from DHHS before printing, production, distribution or use. The DHHS will retain copyright ownership for any and all original materials produced, including, but not limited to, brochures, resource directories, protocols or guidelines, posters, or reports. Contractor shall not reproduce any materials produced under the contract without prior written approval from DHHS. For clarification, Contractor retains ownership of the Software, any portions or copies thereof, and all rights therein other than those granted to the State by this Agreement. Contractor reserves all rights not expressly granted to DHHS. This Agreement does not grant DHHS any rights in connection with any trademarks or service marks of Contractor, its suppliers or licensors. All right, title, interest and copyrights in and to the Software, Documentation and any copies thereof are owned by Contractor, its suppliers or licensors except those created exclusively for the State.
- 1.9 Operation of Facilities: Compliance with Laws and Regulations:** In the operation of any facilities for providing services, the Contractor shall comply with all laws, orders and regulations of federal, state, county and municipal authorities and with any direction of any Public Officer or officers pursuant to laws which shall impose an order or duty upon the contractor with respect to the operation of the facility or the provision of the services at such facility. If any governmental license or permit shall be required for the operation of the said facility or the performance of the said services, the Contractor will procure said license or permit, and will at all times comply with the terms and conditions of each such license or permit. In connection with the foregoing requirements, the Contractor hereby covenants and agrees that, during the term of this Contract the facilities shall comply with all rules, orders, regulations, and requirements of the State Office of the Fire Marshal and the local fire protection agency, and shall be in conformance with local building and zoning codes, by-laws and regulations.
- 1.10 Subcontractors:** DHHS recognizes that the Contractor may choose to use subcontractors with greater expertise to perform for efficiency or convenience, but the Contractor shall retain the responsibility and accountability for the function(s). Prior to subcontracting, the Contractor shall evaluate the subcontractor's ability to perform the delegated function(s). This is accomplished through a written agreement that specifies activities and reporting responsibilities of the subcontractor and provides for revoking the delegation or imposing sanctions if the subcontractor's performance is not adequate. Subcontractors are subject to the same contractual conditions as the Contractor and the Contractor is responsible to ensure subcontractor compliance with those conditions. When the Contractor delegates a function to a subcontractor, the Contractor shall do the following:
- 1.10.1 Evaluate the prospective subcontractor's ability to perform the activities, before delegating the function
 - 1.10.2 Have a written agreement with the subcontractor that specifies activities and reporting responsibilities and how sanctions/revocation will be managed if the subcontractor's performance is not adequate

**STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR NXT HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT - PART 3
EXHIBIT C
SPECIAL PROVISIONS**

- 1.10.3 Monitor the subcontractor's performance on an ongoing basis
- 1.10.4 DHHS shall, at its discretion, review and approve all subcontracts. If the Contractor identifies deficiencies or areas for improvement are identified, the Contractor shall take corrective action.

1.11 Equal Employment Opportunity Plan (EEOP): The Contractor will provide an Equal Employment Opportunity Plan (EEOP) to the Office for Civil Rights, Office of Justice Programs (OCR), if it has received a single award of \$500,000 or more. If the recipient receives \$25,000 or more and has 50 or more employees, it will maintain a current EEOP on file and submit an EEOP Certification Form to the OCR, certifying that its EEOP is on file. For recipients receiving less than \$25,000, or public grantees with fewer than 50 employees, regardless of the amount of the award, the recipient will provide an EEOP Certification Form to the OCR certifying it is not required to submit or maintain an EEOP. Nonprofit organizations, Indian Tribes, and medical and educational institutions are exempt from the EEOP requirement, but are required to submit a certification form to the OCR to claim the exemption. EEOP Certification Forms are available at: <http://www.ojp.usdoj/about/ocr/pdfs/cert.pdf>.

1.12 Limited English Proficiency (LEP): As clarified by Executive Order 13166, Improving Access to Services for persons with Limited English Proficiency (LEP), and resulting agency guidance, national origin discrimination includes discrimination on the basis of LEP. To ensure compliance with the Omnibus Crime Control and Safe Streets Act of 1968 and Title VI of the Civil Rights Act of 1964, Contractors must take reasonable steps to ensure that LEP persons have meaningful access to its programs.

1.13 Pilot Program for Enhancement of Contractor Employee Whistleblower Protections: The following shall apply to all contracts that exceed the Simplified Acquisition Threshold as defined in 48 CFR 2.101 (currently, \$150,000)

**CONTRACTOR EMPLOYEE WHISTLEBLOWER RIGHTS AND REQUIREMENT TO INFORM
EMPLOYEES OF WHISTLEBLOWER RIGHTS (SEP 2013)**

(a) This contract and employees working on this contract will be subject to the whistleblower rights and remedies in the pilot program on Contractor employee whistleblower protections established at 41 U.S.C. 4712 by section 828 of the National Defense Authorization Act for Fiscal Year 2013 (Pub. L. 112-239) and FAR 3.908.

(b) The Contractor shall inform its employees in writing, in the predominant language of the workforce, of employee whistleblower rights and protections under 41 U.S.C. 4712, as described in section 3.908 of the Federal Acquisition Regulation.

(c) The Contractor shall insert the substance of this clause, including this paragraph (c), in all subcontracts over the simplified acquisition threshold.

1.14 SUBPARAGRAPH 4 of the General Provisions of this contract, Conditional Nature of Agreement, is replaced as follows:
4. CONDITIONAL NATURE OF AGREEMENT.

**STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR NXT HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT - PART 3
EXHIBIT C
SPECIAL PROVISIONS**

Notwithstanding any provision of this Agreement to the contrary, all obligations of the State hereunder, including without limitation, the continuance of payments, in whole or in part, under this Agreement are contingent upon continued appropriation or availability of funds, including any subsequent changes to the appropriation or availability of funds affected by any state or federal legislative or executive action that reduces, eliminates, or otherwise modifies the appropriation or availability of funding for this Agreement and the Scope of Services provided in Exhibit A, Scope of Services, in whole or in part. In no event shall the State be liable for any payments hereunder in excess of appropriated or available funds. In the event of a reduction, termination or modification of appropriated or available funds, the State shall have the right to withhold payment until such funds become available, if ever. The State shall have the right to reduce, terminate or modify services under this Agreement immediately upon giving the Contractor notice of such reduction, termination or modification. The State shall not be required to transfer funds from any other source or account into the Account(s) identified in block 1.6 of the General Provisions, Account Number, 05-95-90-902010-5260-102-500731 or any other account, in the event funds are reduced or unavailable.

- 1.15** SUBPARAGRAPH 10 of the General Provisions of this contract, Termination, is amended by adding the following language;

10.1 The State may terminate the Agreement at any time for any reason, at the sole discretion of the State, 30 days after giving the Contractor written notice that the State is exercising its option to terminate the Agreement.

10.2 In the event of early termination, the Contractor shall, within 15 days of notice of early termination, develop and submit to the State a Transition Plan for services under the Agreement, including but not limited to, identifying the present and future needs of clients receiving services under the Agreement and establishes a process to meet those needs.

10.3 The Contractor shall fully cooperate with the State and shall promptly provide detailed information to support the Transition Plan including, but not limited to, any information or data requested by the State related to the termination of the Agreement and Transition Plan and shall provide ongoing communication and revisions of the Transition Plan to the State as requested.

10.4 In the event that services under the Agreement, including but not limited to clients receiving services under the Agreement are transitioned to having services delivered by another entity including contracted providers or the State, the Contractor shall provide a process for uninterrupted delivery of services in the Transition Plan.

10.5 The Contractor shall establish a method of notifying clients and other affected individuals about the transition. The Contractor shall include the proposed communications in its Transition Plan submitted to the State as described above.

- 1.16** Subparagraph 12 of the General Provisions of this contract, Assignment/Delegation/Subcontracts, is replaced as follows;

12. The Contractor shall not assign, or otherwise transfer any interest in this Agreement without the prior written consent of the N.H. Department of Administrative Services. None of the Services shall be subcontracted by the Contractor without the prior written consent of the State. Such consent will not be unreasonably withheld.

- 1.17** Subparagraph 13 of the General Provisions of this contract, Indemnification, is replaced as follows;

**STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR NXT HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT - PART 3
EXHIBIT C
SPECIAL PROVISIONS**

13. INDEMNIFICATION

The Contractor shall defend, indemnify and hold harmless the State, its officers and employees, from and against any and all losses suffered by the State, its officers and employees, and any and all claims, liabilities or penalties asserted against the State, its officers and employees, by or on behalf of any person, on account of, based or resulting from, arising out of (or which may be claimed to arise out of) the negligent or willful acts or omissions of the Contractor. The State shall notify the Contractor in writing, and with reasonable promptness, of any claim, demand, suit, cause of action or legal proceeding that may give rise to a claim against the Contractor for defense. Notwithstanding the foregoing, nothing herein contained shall be deemed to constitute a waiver of the sovereign immunity of the State, which immunity is hereby reserved to the State. This covenant in paragraph 13 shall survive the termination of this Agreement.

- 1.18 EXTENSION** This agreement has the option for a potential extension of up to four (4) additional years, contingent upon satisfactory delivery of services, available funding, agreement of the parties and approval of the Governor and Council.

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR NXT HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT - PART 3
EXHIBIT D
ADMINISTRATIVE SERVICES

1. STATE MEETINGS AND REPORTS

The State believes that effective communication and reporting are essential to Project success.

Airbus Key Project Staff shall participate in meetings as requested by the State, in accordance with the requirements and terms of this Contract.

- a. **Kickoff Meeting:** Participants will include the State and Airbus Project Teams and major stakeholders. This meeting is to establish a sound foundation for activities that will follow.
- b. **Status Meetings:** Participants will include, at the minimum, the Airbus Project Manager and the State Project Manager. During the Implementation Phase, these meetings will be conducted at least every week and address overall the Project status and any additional topics needed to remain on schedule and within budget. A status and error report from Airbus shall serve as the basis for discussion.
- c. **The Work Plan:** must be reviewed at each Status Meeting and updated, at minimum, on a weekly basis, in accordance with the Contract.
- d. **Special Meetings:** Need may arise for a special meeting with State leaders or Project stakeholders to address specific issues.
- e. **Exit Meeting:** Participants will include Project leaders from Airbus and the State. Discussion will focus on lessons learned from the Project and on follow up options that the State may wish to consider.

The State expects Airbus to prepare agendas and background for and minutes of meetings. Background for each status meeting must include an updated Work Plan. Drafting of formal presentations, such as a presentation for the kickoff meeting, will also be Airbus' responsibility.

The Airbus Project Manager or Airbus Key Project Staff shall submit weekly status reports during the Implementation Phase in accordance with the Schedule and terms of this Contract. All status reports shall be prepared in formats approved by the State. The Airbus' Project Manager shall assist the State's Project Manager, or itself produce reports related to Project Management as reasonably requested by the State, all at no additional cost to the State. Airbus shall produce Project status reports, which shall contain, at a minimum, the following:

1. Project status related to the Work Plan;
2. Deliverable status;
3. Accomplishments during weeks being reported;
4. Planned activities for the upcoming one-week period;
5. Future activities; and
6. Issues and concerns requiring resolution.
7. Report and remedies in case of falling behind Schedule

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR NXT HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT - PART 3
EXHIBIT D
ADMINISTRATIVE SERVICES

As reasonably requested by the State, Airbus shall provide the State with information or reports regarding the Project. Airbus shall prepare special reports and presentations relating to Project Management, and shall assist the State in preparing reports and presentations, as reasonably requested by the State, all at no additional cost to the State.

2. STATE-OWNED DOCUMENTS AND DATA

Airbus shall provide the State access to all documents, State Data, materials, reports, and other work in progress relating to the Contract ("State Owned Documents"). Upon expiration or termination of the Contract with the State, Airbus shall turn over all State-owned documents, material, reports, and work in progress relating to the Contract to the State at no additional cost to the State. State-owned Documents must be provided in both printed and electronic format.

3. RECORDS RETENTION AND ACCESS REQUIREMENTS

Airbus shall agree to the conditions of all applicable State and federal laws and regulations, which are incorporated herein by reference, regarding retention and access requirements, including without limitation, retention policies consistent with the Federal Acquisition Regulations (FAR) Subpart 4.7 *Contractor Records Retention*.

Airbus and its Subcontractors shall maintain books, records, documents, and other evidence of accounting procedures and practices, which properly and sufficiently reflect all direct and indirect costs invoiced in the performance of their respective obligations under the Contract, and its Subcontractors shall retain all such records for three (3) years following termination of the Contract, including any extensions. Records relating to any litigation matters regarding the Contract shall be kept for one (1) year following the termination of all litigation, including the termination of all appeals or the expiration of the appeal period.

Upon prior notice and subject to reasonable time frames, all such records shall be subject to inspection, examination, audit and copying by personnel so authorized by the State and federal officials so authorized by law, rule, regulation or Contract, as applicable. Access to these items shall be provided within Merrimack County of the State of New Hampshire, unless otherwise agreed by the State. Delivery of and access to such records shall be at no cost to the State during the three (3) year period following termination of the Contract and one (1) year term following litigation relating to the Contract, including all appeals or the expiration of the appeal period. Airbus shall include the record retention and review requirements of this section in any of its subcontracts.

The State agrees that books, records, documents, and other evidence of accounting procedures and practices related to Airbus' cost structure and profit factors shall be excluded from the State's review unless the cost of any other Services or Deliverables provided under the Contract is calculated or derived from the cost structure or profit factors.

4. ACCOUNTING REQUIREMENTS

Airbus shall maintain an accounting system in accordance with generally accepted accounting principles. The costs applicable to the Contract shall be ascertainable from the accounting system and Airbus shall maintain records pertaining to the Services and all other costs and expenditures.

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR NXT HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT - PART 3
EXHIBIT E
IMPLEMENTATION SERVICES

Airbus shall provide the State with the following services set forth in Contract Exhibit A.

1. IMPLEMENTATION STRATEGY

1.1 Key Components

Airbus shall provide a variety of resources to assist the State in the Implementation of the Communicator. Project Management services shall serve to facilitate communications and maximize efforts emergency of notification System deployments. A Project Manager shall serve as a single point of contact and primary Project Facilitator for all related issues during the Implementation period through Acceptance. Airbus uses a phased approach to Project Implementation.

1.2 Phase I – Planning

Phase I is the period of time which the Project is formally launched, the Project design is finalized, a Work Plan is created and resources are scheduled. The Project Manager shall coordinate Phase I activities with the State to ensure the Project scope has been assessed, and that all Deliverables have been integrated into a comprehensive Master Project Schedule that will be attached to the Work Plan. The Work Plan shall be the control document for Deliverables for the Implementation as well as other critical dates or milestones that are integral to the Project. Critical activities within Phase I shall include:

1.2.1 Kickoff Meeting Call

- a. Scheduled 5 days after Contract approval
- b. Process owners are identified
- c. Key Project milestones and objectives are introduced and discussed.
- d. Review the overall Project "As Purchased" design.
- e. First review of the draft Work Plan.

1.2.2 Phase I Planning Meeting

- a. Within 5 days of the Project launch.
- b. Detailed Review of the "As Purchased" System design.
- c. Work Plan Approval

1.2.3 Project Schedule

- a. Resources will be scheduled and communicated to the team members via the Master Project Schedule.
- b. The Master Schedule will be drafted and forwarded to team members for review and comment.
- c. This "first pass" schedule will be used to present the initial deployment schedule.
- d. Once all feedback and changes have been received and integrated into the schedule, the Master Schedule will be published by the Project Manager.
- e. Once published, the Master Schedule will only be changed as per appropriately submitted change requests.

**STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR NXT HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT - PART 3
EXHIBIT E
IMPLEMENTATION SERVICES**

1.2.3 Work Plan Approval

- a. The Work Plan has been approved.
- b. System design is completed.

1.3 Phase II – Implementation

Phase II is the period of time in which System Implementation and training take place. The Project's Implementation is accomplished to the degree that is possible without actually going live. The Project Manager shall coordinate the Phase II activities with the State to minimize interference with other site activities, while ensuring that the Implementation and Training are completed as part of the Work Plan and the Master Project Schedule.

1.3.1 Implementation and Training milestones and Deliverables will be documented and managed via the Master Project Schedule. The Installation Responsibility Matrix delineates task level responsibilities for installation.

1.3.2 Complete hosting set up:

- a. Hosting set-up is complete.
- b. Training has been completed to the degree agreed upon during the Project Planning Process.
- c. Testing is complete.

1.4 Phase III – Cutover Phase

The Cutover phase defines any Deliverables required in the Implementation Phase, but not satisfied. If any such issues exist, the System will be placed in a locked down state. Once these issues are identified and agreed upon, the Project Manager will facilitate the completion of those items are services. Once all items have been completed, the Project and Software Acceptance is signed and the System will be unlocked and turned over to the customer.

1.5 Phase IV – Post Cut and Support

The Post Cut and Support Phase shall occur when the Project and Software Acceptance has been signed. Its purpose is to ensure immediate technical support to the State if necessary. Any additional Training or other services purchased, but not accomplished during the Implementation Phase, will be addressed in this Phase. In this phase, your Project Manager will transition the Project to Technical Services. This will end the Project Manager's involvement on this Project.

1.5.1 Snapshot

This is a basic overview/snapshot of the steps taken for a smooth transition for a State-hosted to a Vendor-hosted System. These steps only apply to a Communicator 4.2.1 to 4.4 Conversion.

- a. Obtain Communicator information from the State
- b. Submit requests to Infrastructure
- c. Set up an agreed time for Cut-Over and Migrate Database and Reports (if desired)

1.5.2 Pre-Upgrade Backups:

**STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR NXT HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT - PART 3
EXHIBIT E
IMPLEMENTATION SERVICES**

- a. Run DB Snapshot
- b. Backup Call Flows
- c. Backup Import Files
- d. Backup Pager Scripts
- e. Backup Databases
- f. Create listing of Company Maintenance Settings
- g. Move all backups to FTP Site

1.5.3 Data Migration:

- a. Data freeze
- b. Get snapshot of current database
- c. Upgrade to v4.4.2
- d. Setup Paging/SMS
- e. Test Company to ensure devices working
- f. Add Company to DataSync
- g. Remove scheduled activation scenario settings
- h. Get snapshot of upgraded database

1.5.4 Test Primary Server:

- a. Compare snapshot of data for data integrity
- b. Test scenarios - existing and new - Users will receive System reports
- c. Test messages - existing and new
- d. Test groups - existing and new
- e. Check Security Users
- f. Check scenarios and group Security Users
- g. Test paging/SMS
- h. Test email and email response
- i. Test call transfer
- j. Test conference bridge

1.5.5 Primary System Acceptance:

- a. Finalize the State's configurations
- b. Coordinate training dates

1.5.6 Version 4.4 Backup System:

- a. Set up DataSync on backup

1.5.7 Move DataSync from Onsite Backup to v4.4.2 Backup:

- a. Infrastructure request to move existing backup URL and phone numbers to v4.4.2
- b. Complete Project documentation
- c. Send URL, Login, and System access information to the State
- d. Discontinue DataSync from State-hosted server

**STATE OF NEW HAMPSHIRE
DEPATMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR NXT HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT - PART 3
EXHIBIT E
IMPLEMENTATION SERVICES**

1.6 Phase V – Production

- a. Version 4.4.2 Primary & Backup Server In Production

**STATE OF NEW HAMPSHIRE
DEPATMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR NXT HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT - PART 3
EXHIBIT E-1
SECURITY AND INFRASTRUCTURE**

1. SECURITY

Airbus shall ensure that appropriate levels of security are implemented and maintained in order to protect the integrity and reliability of the State's Data. Security requirements are defined in the Requirements in Exhibit H.

**STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR NXT HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT - PART 3
EXHIBIT F
TESTING SERVICES**

Airbus shall provide the following Products and Services described in this Exhibit F, including but not limited to:

1. TESTING AND ACCEPTANCE

Airbus shall bear all responsibilities for the full suite of Test Planning and preparation throughout the Project. Airbus will also provide training as necessary to the State staff responsible for test activities. Airbus shall be responsible for all aspects of testing contained in the Acceptance Test Plan including support, at no additional cost, during User Acceptance Test conducted by the State and the testing of the training materials.

The Test Plan methodology shall reflect the needs of the Project and be included in the finalized Work Plan. A separate Test Plan and set of test materials will be prepared for each Software function or module.

All Testing and Acceptance (both business and technically oriented testing) shall apply to testing the System as a whole, (e.g., software modules or functions, and Implementation(s)). This shall include planning, test scenario and script development, Data and System preparation for testing, and execution of Unit Tests, System Integration Tests, Conversion Tests, Installation tests, Regression tests, Performance Tuning and Stress tests, Security Review and tests, and support of the State during User Acceptance Test and Implementation.

In addition, Airbus shall provide a mechanism for reporting actual test results vs. expected results and for the resolution and tracking of all errors and problems identified during test execution. Airbus shall also correct Deficiencies and support required re-testing.

1.1 Test Planning and Preparation

Airbus shall provide the State with an overall Test Plan that will guide all testing. The Airbus provided, State approved, Test Plan will include, at a minimum, identification, preparation, and Documentation of planned testing, a requirements traceability matrix, test variants, test scenarios, test cases, test scripts, test Data, test phases, unit tests, expected results, and a tracking method for reporting actual versus expected results as well as all errors and problems identified during test execution.

As identified in the Acceptance Test Plan, and documented in accordance with the Work Plan and the Contract, State testing will commence upon Airbus' Project Manager's Certification, in writing, that Airbus' own staff has successfully executed all prerequisite Airbus testing, along with reporting the actual testing results, prior to the start of any testing executed by State staff. The State will be presented with a State approved Acceptance Test Plan, test scenarios, test cases, test scripts, test data, and expected results.

The State will commence its testing within 5 business days of receiving Certification from Airbus that the State's personnel have been trained and the System is installed, configured, complete, and ready for State testing. The testing will be conducted by the State in an environment independent from Airbus' development environment. Airbus must assist the State with testing in accordance

**STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR NXT HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT - PART 3
EXHIBIT F
TESTING SERVICES**

with the Test Plan and the Work Plan, utilizing test and live Data to validate reports, and conduct stress and performance testing, at no additional cost.

Testing begins upon completion of the Software configuration as required and user training according to the Work Plan. Testing ends upon issuance of a letter of User Acceptance Testing (UAT) Acceptance by the State.

Vendor must demonstrate that their testing methodology can be integrated with the State standard methodology.

1.2 UAT

UAT begins upon completion of the Software configuration as required and user training according to the Work Plan. Testing ends upon issuance of a letter of UAT Acceptance by the State.

The Vendor's Project Manager must certify in writing, that the Vendor's own staff has successfully executed all prerequisite Vendor testing, along with reporting the actual testing results prior to the start of any testing executed by State staff.

The State shall be presented with all testing results, as well as written Certification that Airbus has successfully completed the prerequisite tests, meeting the defined Acceptance Criteria, and performance standards. The State shall commence testing within five (5) business days of receiving Certification, in writing, from Airbus that the system is installed, configured, complete and ready for State testing. The State shall conduct the UAT utilizing scripts developed as identified in the Acceptance Test Plan to validate the functionality of the System and the interfaces, and verify Implementation readiness. UAT is performed in a copy of the production environment and can serve as a performance and stress test of the System. The UAT may cover any aspect of the new System, including administrative procedures (such as backup and recovery).

The UAT is a verification process performed in a copy of the production environment. The UAT verifies System functionality against predefined Acceptance criteria that support the successful execution of approved business processes.

UAT will also serve as a performance and stress test of the System. It may cover any aspect of the new System, including administrative procedures such as backup and recovery. The results of the UAT provide evidence that the new System meets the User Acceptance criteria as defined in the Work Plan.

The results of the UAT provide evidence that the new System meets the User Acceptance criteria as defined in the Work Plan.

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR NXT HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT - PART 3
EXHIBIT F
TESTING SERVICES

Upon successful conclusion of UAT and successful System deployment, the State will issue a letter of UAT Acceptance and the respective Warranty Period shall commence.

	The System User Acceptance Tests verify System functionality against predefined Acceptance criteria that support the successful execution of approved processes.
	<ul style="list-style-type: none">• Provide the State an Acceptance Test Plan and selection of test scripts for the Acceptance Test.• Monitor the execution of the test scripts and assist as needed during the User Acceptance Test activities.• Work jointly with the State in determining the required actions for problem resolution.
	<ul style="list-style-type: none">• Approve the development of the User Acceptance Test Plan and the set of data for use during the User Acceptance Test.• Validate the Acceptance Test environment.• Execute the test scripts and conduct User Acceptance Test activities.• Document and summarize Acceptance Test results.• Work jointly with Airbus in determining the required actions for problem resolution.• Provide Acceptance of the validated Systems.
	The Deliverable for User Acceptance Tests is the User Acceptance Test Results. These results provide evidence that the new System meets the User Acceptance criteria defined in the Work Plan.

1.3 Regression Testing

As a result, of the user testing activities, problems will be identified that require correction. The State will notify the Vendor of the nature of the testing failures in writing. The Vendor will be required to perform additional testing activities in response to State and/or user problems identified from the testing results. Regression testing means selective re-testing to detect faults introduced during the modification effort, both to verify that the modifications have not caused unintended adverse effects, and to verify that the modified and related (possibly affected) System components still meet their specified requirements:

- a. For each minor failure of an Acceptance Test, the Acceptance Period shall be extended by corresponding time defined in the Test Plan.
- b. Airbus shall notify the State no later than 5 business days from the Airbus' receipt of written notice of the test failure when Airbus expects the corrections to be completed and ready for retesting by the State. Airbus will have up to five (5) business days to make corrections to the problem unless specifically extended in writing by the State.
- c. When a programming change is made in response to a problem identified during user testing, a Regression Test Plan should be developed by Airbus based on the understanding of the

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR NXT HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT - PART 3
EXHIBIT F
TESTING SERVICES

program and the change being made to the program. The Regression Test Plan has two objectives:

1. Validate that the change/update has been properly incorporated into the program; and
 2. Validate that there has been no unintended change to the other portions of the program.
- d. Airbus will be expected to:
1. Create a set of test conditions, test cases, and test data that will validate that the change has been incorporated correctly;
 2. Create a set of test conditions, test cases, and test data that will validate that the unchanged portions of the program still operate correctly; and
 3. Manage the entire cyclic process.
- e. Airbus will be expected to execute the regression test, provide actual testing results, and certify its completion in writing to the State prior to passing the modified Software application to the users for retesting.

In designing and conducting such regression testing, Airbus will be required to assess the risks inherent to the modification being implemented and weigh those risks against the time and effort required for conducting the regression tests. In other words, Airbus will be expected to design and conduct regression tests that will identify any unintended consequences of the modification while taking into account Schedule and economic considerations.

1.4 Security Review and Testing

IT Security involves all functions pertaining to the securing of State Data and Systems through the creation and definition of security policies, procedures and controls covering such areas as identification, authentication and non-repudiation.

All components of the Software shall be reviewed and tested to ensure they protect the State's Data assets.

Tests shall focus on the technical, administrative and physical security controls that have been designed into the System architecture in order to provide the necessary confidentiality, integrity and availability. Tests shall, at a minimum, cover each of the service components. Test procedures may include Penetration Tests (pen test) or code analysis and Review.

Service Component	Defines the set of capabilities that:
Identification and Authentication	Supports obtaining information about those parties attempting to log onto a System or application for security purposes and the validation of users
Access Control	Supports the management of permissions for logging onto a computer or network
Encryption	Supports the encoding of data for security purposes

**STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR NXT HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT - PART 3
EXHIBIT F
TESTING SERVICES**

Intrusion Detection	Supports the detection of illegal entrance into a computer system
Verification	Supports the confirmation of authority to enter a computer system, application or network
Digital Signature	Guarantees the unaltered state of a file
User Management	Supports the administration of computer, application and network accounts within an organization.
Role/Privilege Management	Supports the granting of abilities to users or groups of users of a computer, application or network
Audit Trail Capture and Analysis	Supports the identification and monitoring of activities within an application or System
Input Validation	Ensures the application is protected from buffer overflow, cross-site scripting, SQL injection, and unauthorized access of files and/or directories on the server.

Airbus acknowledges its responsibility for security testing. Tests shall focus on the technical, administrative and physical security controls that have been designed into the System architecture in order to provide the necessary confidentiality, integrity and availability. Tests shall, at a minimum, cover each of the service components. Test procedures shall include 3rd party Penetration Tests (pen test) or code analysis and review.

Prior to the System being moved into production, Airbus shall provide results of all security testing to the DHHS for review and Acceptance. All Software and hardware shall be free of malicious code (Malware).

1.5 Successful UAT Completion

Upon successful completion of UAT, the State will issue a Letter of UAT Acceptance. Upon issuance of the Letter of UAT Acceptance by the State, the respective Warranty Period shall commence as set forth in Contract Exhibit K: *Warranty and Warranty Services*.

1.6 System Acceptance

After 30 days of fault free operation (after flash cut to hosted System), the State shall issue a letter of Final System Acceptance.

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR NXT HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT - PART 3
EXHIBIT G
MAINTENANCE AND SUPPORT SERVICES

1. SYSTEM MAINTENANCE

Airbus shall maintain and support the System in all material respects as described in the applicable program Documentation for five (5) years of maintenance after User Acceptance and successful completion of the Warranty Period of sixty (60) months.

1.1 Airbus DS Communications, Inc.'s Responsibility

Airbus shall maintain the Application System in accordance with the Contract. Airbus will not be responsible for maintenance or support for Software developed or modified by the State.

1.1.1 Maintenance Releases

Airbus shall make available to the State the latest program updates, general maintenance releases, selected functionality releases, patches, and Documentation that are generally offered to its customers, at no additional cost.

2. SYSTEM SUPPORT

2.1 Airbus DS Communications Inc.'s Responsibility

Airbus will be responsible for performing on-site or remote technical support in accordance with the Contract Documents, including without limitation the requirements, terms, and conditions contained herein.

As part of the Software maintenance agreement, ongoing Software maintenance and support levels, including all new Software releases, shall be responded to according to the following:

- a. **Class A Deficiencies** - The Vendor shall have available to the State email and on-call telephone assistance, with issue tracking available to the State, twenty-four (24) hours per day and seven (7) days a week with an email / telephone response within two (2) hours of request;
- b. **Class B Deficiencies** -The State shall notify the Vendor of such Deficiencies during regular business hours and the Vendor shall respond back within seventy-two (72) hours of notification of planned corrective action;
- c. **Class C Deficiencies** -The State shall notify the Vendor of such Deficiencies during regular business hours and the Vendor shall respond back within four (4) business days of notification of planned corrective action;

3. SUPPORT OBLIGATIONS AND TERM

- 3.1 Airbus shall repair or replace Software, and provide maintenance of the Software in accordance with the Specifications and terms and requirements of the Contract;
- 3.2 Airbus shall maintain a record of the activities related to warranty repair or maintenance activities performed for the State;
- 3.3 For all maintenance Services calls, Airbus shall ensure the following information will be collected and maintained: 1) nature of the Deficiency; 2) current status of the Deficiency; 3) action plans,

Contract 2015-049 Agreement – Part 3 Exhibit G-Maintenance and Support Services

Initial and Date All Pages:

Airbus Initials AC

Date: 7-11-2015

**STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR NXT HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT - PART 3
EXHIBIT G
MAINTENANCE AND SUPPORT SERVICES**

dates, and times; 4) expected and actual completion time; 5) Deficiency resolution information, 6) Resolved by, 7) Identifying number i.e. work order number, 8) Issue identified by; and

- 3.4 Airbus must work with the State to identify and troubleshoot potentially large-scale System failures or Deficiencies by collecting the following information: 1) mean time between reported Deficiencies with the Software; 2) diagnosis of the root cause of the problem; and 3) identification of repeat calls or repeat Software problems.
- 3.5 If Airbus fails to correct a Deficiency within the allotted period of time stated above, Airbus shall be deemed to have committed an Event of Default, and the State shall have the right, at its option, to pursue the remedies in Part 2 Section 13, Termination, as well as to return Airbus' product and receive a refund for all amounts paid to Airbus, including but not limited to, applicable license fees, within ninety (90) days of notification to Airbus of the State's refund request
- 3.6 If Airbus fails to correct a Deficiency within the allotted period of time Stated above, Airbus shall be deemed to have committed an Event of Default, and the State shall have the right, at its option, to pursue the remedies in Part 2 Section 13, Termination.

**STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR NXT HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT - PART 3
EXHIBIT H
REQUIREMENTS**

The Requirements are attached (Attachment 2).

**STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR NXT HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT - PART 3
EXHIBIT I
WORK PLAN**

Airbus' Project Manager and the State Project Manager shall finalize the Work Plan within five days of the Effective Date and further refine the tasks required to Implement the Project. The elements of the preliminary Work Plan are documented in accordance with Airbus' plan to Implement the Application Software. Continued development and management of the Work Plan is a joint effort on the part of Airbus and State Project Managers.

The preliminary Work Plan created by Airbus and the State is set forth at the end of this Exhibit.

In conjunction with Airbus' Project Management methodology, which shall be used to manage the Project's life cycle, the Airbus team and the State shall finalize the Work Plan at the onset of the Project. This plan shall identify the tasks, Deliverables, major milestones, task dependencies, and a payment Schedule required to Implement the Project. It shall also address intra-task dependencies, resource allocations (both State and Airbus team members), refine the Project's scope, and establish the Project's Schedule. The Plan is documented in accordance with Airbus' Work Plan and shall utilize MS Project and/or MS Excel to support the ongoing management of the Project.

1. ASSUMPTIONS

1.1 General

- a. The State shall provide team members with decision-making authority to support the Implementation efforts.
- b. All State tasks must be performed in accordance with the revised Work Plan.
- c. All key decisions will be resolved within five (5) business days. Issues not resolved within this initial period will be escalated to the State Project Manager for resolution.
- d. Any activities, decisions or issues taken on by the State that affect the mutually agreed upon Work Plan timeline, scope, resources, and costs shall be subject to the identified Change Control process.
- e. Airbus shall maintain an accounting system in accordance with Generally Accepted Accounting Principles (GAAP).

1.2 Logistics

- a. The Airbus Team shall perform this Project at the Airbus's facilities.
- b. The Airbus Team shall honor all holidays observed by Airbus or the State, although with permission, may choose to work on holidays and weekends.

1.3 Project Management

- a. The State shall provide the Project Team with reasonable access to the State personnel as needed to complete Project tasks.
- b. A Project folder created within the State System shall be used for centralized storage and retrieval of Project documents, work products, and other material and information relevant to the success of the Project and required by Project Team members. This central repository is secured by determining which team members have access to the Project folder and granting either view or read/write privileges. The State Project Manager will establish and maintain this folder. The State Project Manager shall approve access for the State team. Documentation can be stored locally for Airbus and State team on a "shared" network drive to facilitate ease and speed of access. Final versions of all Documentation shall be loaded to the State System.
- c. Airbus assumes that an Alternate Project Manager may be appointed from time to time to handle reasonable and ordinary absences of the Project Manager.

**STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR NXT HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT - PART 3
EXHIBIT I
WORK PLAN**

1.4 Technical Environment and Management

- The State is responsible for providing the Internet access.

1.5 Conversions

- The Airbus Team's proposal is based on the assumption that the State's technical team is capable of implementing, with assistance from the Airbus technical team, a subset of the conversions. The Airbus Team shall lead the State with the mapping of the legacy Data to the Airbus applications.

1.6 Project Schedule

- Deployment is planned to begin on the date of Governor and Council approval with a planned go-live date of 6 to 8 weeks later.

1.7 Reporting

- Airbus shall conduct weekly status meetings, and provide reports that include, but are not limited to, minutes, action items, test results and Documentation during the Implementation Phases I - V.

1.8 User Training and Change Management

- The Airbus Team shall lead the development of the end-user training plan.
- Airbus is responsible for the delivery of end-user training.
- The State shall schedule and track attendance on all end-user training classes.

1.9 Performance and Security Testing

- The Airbus Team shall provide a performance test workshop to identify the key scenarios to be tested, the approach and tools required, and best practices information on performance testing.
- The State shall work with Airbus on performance testing as set forth in Contract Exhibit F – *Testing Services*.

2. ROLES AND RESPONSIBILITIES

2.1 Airbus DS Communications, Inc. Team Roles and Responsibilities

2.1.1 Airbus DS Communications, Inc. Team Project Manager

The Airbus Team Project Manager shall have overall responsibility for the day-to-day management of the Project and shall plan, track, and manage the activities of the Airbus Implementation Team. The Airbus Team Project Manager will have the following responsibilities:

- Maintain communications with the State's Project Manager;
- Work with the State in planning and conducting a kick-off meeting;
- Create and maintain the Work Plan;
- Assign Airbus Project Team consultants to tasks in the Implementation Project according to the scheduled staffing requirements;
- Define roles and responsibilities of all Airbus Team members;
- Provide every two weeks and month update progress reports to the State Project Manager;

**STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR NXT HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT - PART 3
EXHIBIT I
WORK PLAN**

- Notify the State Project Manager of requirements for State resources in order to provide sufficient lead time for resources to be made available;
- Review task progress for time, quality, and accuracy in order to achieve progress;
- Review requirements and scheduling changes and identify the impact on the Project in order to identify whether the changes may require a change of scope;
- Implement scope and Schedule changes as authorized by the State Project Manager and with appropriate Change Control approvals as identified in the Implementation Plan;
- Inform the State Project Manager and staff of any urgent issues if and when they arise;
- Provide the State completed Project Deliverables and obtain sign-off from the State's Project Manager.

2.1.2 Airbus Team Analysis

The Airbus Team shall conduct analysis of requirements, validate the Airbus Team's understanding of the State business requirements by application, and perform business requirements mapping:

- Construct and confirm application test case scenarios;
- Produce application configuration definitions and configure the applications;
- Conduct testing of the configured application;
- Produce functional Specifications for extensions, conversions, and interfaces;
- Assist the State in the testing of extensions, conversions, and interfaces;
- Assist the State in execution of the State's Acceptance Test;
- Conduct follow-up meetings to obtain feedback, results, and concurrence/approval from the State;
- Assist with the correction of configuration problems identified during System, integration and Acceptance Testing; and
- Assist with the transition to production.

2.1.3 Airbus Team Tasks

The Airbus team shall assume the following tasks:

- Development and review of functional and technical Specification to determine that they are at an appropriate level of detail and quality;
- Development and Documentation of conversion and interface programs in accordance with functional and technical Specifications;
- Development and Documentation of installation procedures; and
- Development and execution of unit test scripts;
- Unit testing of conversions and interfaces developed; and
- System Integration Testing.

2.2 State Roles and Responsibilities

The following State resources have been identified for the Project. The time demands on the individual State team members will vary depending on the phase and specific tasks of the Implementation. The demands on the Subject Matter Experts' (SME) time will vary based on the need determined by the State Leads and the phase of the Implementation.

**STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR NXT HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT - PART 3
EXHIBIT I
WORK PLAN**

2.2.1 State Project Manager

The State Project Manager shall work side-by-side with the Airbus Project Manager. The role of the State Project Manager is to manage State resources (if any), facilitate completion of all tasks assigned to State staff, and communicate Project status on a regular basis. The State Project Manager represents the State in all decisions on Implementation Project matters, provides all necessary support in the conduct of the Implementation Project, and provides necessary State resources, as defined by the Work Plan and as otherwise identified throughout the course of the Project. The State Project Manager has the following responsibilities:

- Plan and conduct a kick-off meeting with assistance from the Airbus team;
- Assist the Airbus Project Manager in the development of a detailed Work Plan;
- Identify and secure the State Project Team members in accordance with the Work Plan;
- Define roles and responsibilities of all State Project Team members assigned to the Project;
- Identify and secure access to additional State end-user staff as needed to support specific areas of knowledge if and when required to perform certain Implementation tasks;
- Communicate issues to State management as necessary to secure resolution of any matter that cannot be addressed at the Project level;
- Inform the Airbus Project Manager of any urgent issues if and when they arise; and
- Assist the Airbus team staff to obtain requested information if and when required to perform certain Project tasks.

2.2.2. State Subject Matter Expert(s) (SME)

The role of the State SME is to assist application teams with an understanding of the State's current business practices and processes, provide agency knowledge, and participate in the Implementation. Responsibilities of the SME include the following:

- Be the key user and contact for their Agency or Department;
- Attend Project Team training and acquire in-depth functional knowledge of the relevant applications;
- Assist in validating and documenting user requirements, as needed;
- Assist in mapping business requirements;
- Assist in constructing test scripts and data;
- Assist in System, integration, and Acceptance Testing;
- Assist in performing conversion and integration testing and data verification;
- Attend Project meetings when requested; and
- Assist in training end users in the use of the Airbus Software and the business processes the application supports.

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR NXT HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT - PART 3
EXHIBIT I
WORK PLAN

3 SOFTWARE APPLICATION

The software required is described more fully in Exhibit B.

4 CONVERSIONS

Airbus has full access to the State's mirrored System located at Airbus Data Center; therefore, conversions (if any) are the responsibility of the Airbus Project Management Team.

5 PRELIMINARY WORK PLAN

The following Table 5.1 provides the preliminary agreed upon Work Plan for the Contract. The Finalized Work Plan to be completed 10 days after the Governor and Executive Council approval as describe above in Table 1.1.1 – Deliverable Payment Schedule.

Table 5.1: High Level Preliminary NH Work Plan

Task Name	Duration	Start	Finish
Kickoff Meeting	1 hour	August 15, 2015	August 15, 2015
Review, Update and Finalize Preliminary Work Plan	1 hour	August 15, 2015	August 15, 2015
Status Meetings and Reports	weekly	August 15, 2015	10/1/2015
Get NXT info from Customer. <ul style="list-style-type: none"> ✓ Submit requests to Infrastructure. ✓ Set up an agreed time for Cut-Over and Migrate Database and Reports (if desired) 	1½ weeks depending on response from customer		
Pre-Upgrade Backups: <ul style="list-style-type: none"> ✓ Run DB Snapshot ✓ Backup Call Flows ✓ Backup Import Files ✓ Backup Pager Scripts ✓ Backup Databases ✓ Create listing of Company Maintenance Settings ✓ Move all backups to FTP Site 	3 Hours		
Data Migration: <ul style="list-style-type: none"> ✓ Data freeze ✓ Get snapshot of current database 	2 weeks		

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR NXT HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT - PART 3
EXHIBIT I
WORK PLAN

<ul style="list-style-type: none"> ✓ Upgrade to v4.4 ✓ Migrate 4.2.1 databases to v4.4 ✓ Move DB/Callflow backups ✓ Perform Data Migration Steps for database ✓ Import Callflows ✓ Setup Paging/SMS ✓ Test Company to ensure devices working ✓ Add Company to DataSync ✓ Remove scheduled activation scenario settings ✓ Get snapshot of upgraded database 			
Test Primary Server: <ul style="list-style-type: none"> ✓ Compare Snapshot of data for data integrity ✓ Test Scenarios - Existing and New - Users will receive Activation Reports ✓ Test Messages - Existing and New ✓ Test Groups - Existing and New ✓ Check Security Users ✓ Check Scenario and Group Security Users ✓ Test Paging/SMS ✓ Test Email and Email Qualification ✓ Test Call Transfer (if applicable) 	5 Days		
Primary System Acceptance <ul style="list-style-type: none"> ✓ Finalize customer configurations ✓ Coordinate training dates (if applicable) 	3 Days		
4.4 Backup System: <ul style="list-style-type: none"> ✓ Set up DataSync on backup 	3 Hours		
Move DataSync From Onsite Backup to v4.4 Backup: <ul style="list-style-type: none"> ✓ Infrastructure request to move existing backup URL and phone numbers to v4.4 ✓ Complete project documentation ✓ Send URL, Login, and system access information to customer ✓ Stop DataSync from on-premise server 	6 Hours		
v4.4 Primary & Backup Server In Production			
Project Close Out meeting	10/1/2015	10/1/2015	10/1/2015

Contract 2015-049 Agreement – Part 3 Exhibit I Work Plan

Initial and Date All Pages:

Airbus Initials PC

Date: 7-21-2015

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR NXT HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT - PART 3
EXHIBIT I
WORK PLAN

Final System Acceptance by State	10/1/2015	10/1/2015	10/1/2015
User Training and Materials (Year 2)	Includes any pre-purchased training options plus an in-house training seat, or a live webinar of your choice for up to 10 people	10/1/2015	9/30/2017
User Training and Materials (Year 3)	Includes any pre-purchased training options plus an in-house training seat, or a live webinar of your choice for up to 10 people	10/1/2017	9/30/2018
User Training and Materials (Year 4)	Includes any pre-purchased training options plus an in-house training seat, or a live webinar of your choice for up to 10 people	10/1/2018	9/30/2019
User Training and Materials (Year 5)	Includes any pre-purchased training options plus an in-house training seat, or a live webinar of your choice for up to 10 people	10/1/2019	9/30/2020
On-going System Support and Maintenance (Year 1)	The term of the Support Plan will commence with the Effective Date of the Service Agreement and will continue through the Initial Term and any Renewal Terms.	10/1/2015	9/30/2016
On-going System Support and Maintenance (Year 2)	The term of the Support Plan will commence with the Effective Date of the Service Agreement and will continue through the	10/1/2016	9/30/2017

Contract 2015-049 Agreement – Part 3 Exhibit I Work Plan

Initial and Date All Pages:

Airbus Initials pc

Date: 7-21-2015

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR NXT HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT - PART 3
EXHIBIT I
WORK PLAN

	Initial Term and any Renewal Terms.		
On-going System Support and Maintenance (Year 3)	The term of the Support Plan will commence with the Effective Date of the Service Agreement and will continue through the Initial Term and any Renewal Terms.	10/1/2017	9/30/2018
On-going System Support and Maintenance (Year 4)	The term of the Support Plan will commence with the Effective Date of the Service Agreement and will continue through the Initial Term and any Renewal Terms.	10/1/2018	9/30/2019
On-going System Support and Maintenance (Year 5)	The term of the Support Plan will commence with the Effective Date of the Service Agreement and will continue through the Initial Term and any Renewal Terms.	10/1/2019	9/30/2020

**STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR NXT HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT - PART 3
EXHIBIT J
SOFTWARE LICENSE**

1. License

Airbus hereby grants the State a non-exclusive, non-transferable, worldwide term license with the right to use the Service, solely for the State's internal business purposes, subject to the terms and conditions of this Agreement. All rights not expressly granted to The State are reserved by Airbus and its licensors.

2. Access

The State and Airbus shall agree upon, prior to State's use of the Service, the offices and Users authorized to access the Service and such Users shall be identified in writing in advance by the State. The State may modify the list of Users of the Service by providing advance written notice to Airbus. The State may authorize access for the number of simultaneous, concurrent Users of the Service allowed under the Agreement at any given time. Passwords provided for Service access may be used only by authorized personnel. Neither the State nor its authorized personnel shall divulge, sublicense, assign or transfer to any third party passwords established for access to the Service. The State shall be responsible for the confidentiality and security of its User identifications and passwords.

3. The State Responsibilities

The State is responsible for all activity occurring in its User accounts and shall abide by all applicable local, state, federal law and regulations in connection with the State's use of the Service, including but not limited to data privacy, security, international communications and the transmission of technical or personal data. The State shall: (i) Prevent unauthorized access to the Service and notify Airbus immediately of any unauthorized use of any password or account or any other known or suspected breach of security; (ii) report to Airbus immediately and use reasonable efforts to stop immediately any copying or distribution of Content that is known or suspected by the State; and (iii) ensure that use of the Service by all of the State's Users is in compliance with this Agreement.

4. Restrictions

The State shall not (i) license, sublicense, sell, resell, transfer, assign, distribute or otherwise commercially exploit or make available to any third party the Service or the Content in any way; (ii) modify or make derivative works based upon the Service or the Content; (iii) create Internet "links" to the Service or "frame" or "mirror" any Content on any other server or wireless or Internet-based device; (iv) send spam or otherwise duplicative or unsolicited messages in violation of applicable law; (v) send or store infringing, obscene, threatening, libelous, or otherwise unlawful or tortuous material, including material harmful to children or violative of third party privacy rights; (iv) send or store material containing software viruses, worms, Trojan horses or other harmful computer code, files, scripts, agents or programs; (vii) interfere with or disrupt the integrity or performance of the Service or the data contained therein, including but not limited to the State Data; (viii) attempt to gain unauthorized access to the Service or its related Systems or networks; (ix) reverse engineer or access the Service in order to (a) build a competitive product or service, (b) build a product using similar ideas, features, functions or graphics of the Service, or (c) copy any ideas, features, functions or graphics of the Service.

**STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR NXT HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT - PART 3
EXHIBIT K
WARRANTY AND WARRANTY SERVICES**

1. WARRANTIES

1.1 System

Airbus warrants that the System will operate to conform to the Specifications, terms, and requirements of the Contract.

1.2 Software

Airbus warrants that the Software, including but not limited to the individual modules or functions furnished under the Contract, is properly functioning within the System, compliant with the requirements of the Contract, and will operate in accordance with the Specifications and Terms of the Contract.

For any breach of the System or Software Support warranty, the State's remedy, and Airbus' entire liability, shall be: (a) the correction of program errors that cause breach of the warranty, or if Airbus cannot substantially correct such breach in a commercially reasonable manner, the State may end its program license and recover the fees paid to Airbus for the program license and any unused, prepaid technical support fees the State has paid for the program license; or (b) the re-performance of the Deficient services, or (c) if Airbus cannot substantially correct a breach in a commercially reasonable manner, the State may end the relevant services and recover the fees paid to Airbus for the Deficient services.

1.3 Non-Infringement

Airbus warrants that it has good title to, or the right to allow the State to use, all Services, equipment, and Software ("Material") provided under this Contract, and that such Services, equipment, and Software do not violate or infringe any patent, trademark, copyright, trade name or other intellectual property rights or misappropriate a trade secret of any third party.

1.4 Viruses; Destructive Programming

Airbus warrants that the Software shall not contain any viruses, destructive programming, or mechanisms designed to disrupt the performance of the Software in accordance with the Specifications.

1.5 Compatibility

Airbus warrants that all System components, including but not limited to the components provided, including any replacement or upgraded System Software components provided by Airbus to correct Deficiencies or as an Enhancement, shall operate with the rest of the System without loss of any functionality.

1.6 Services

Airbus warrants that all Services to be provided under the Contract will be provided expediently, in a professional manner, in accordance with industry standards and that Services will comply with performance standards, Specifications, and terms of the Contract.

**STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR NXT HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT - PART 3
EXHIBIT K
WARRANTY AND WARRANTY SERVICES**

1.7 Personnel

Airbus warrants that all personnel engaged in the Services shall be qualified to perform the Services, and shall be properly licensed and otherwise authorized to do so under all applicable laws.

1.8 Breach of Data

Airbus shall be solely liable for costs associated with any breach of State data housed at their location(s) including but not limited to notification and any damages assessed by the courts.

2. WARRANTY PERIOD

All warranties shall remain in effect for the duration of the contract and any extensions, with the exception of the warranty for non-infringement which shall survive the termination of this agreement.

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR NXT HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT - PART 3
EXHIBIT L
TRAINING SERVICES

Airbus shall provide the following Training Services.

1. TRAINING

There are three training options available:

1. Delivery Method – Two-day, Onsite, Instructor-Led Class Training

A member of the Airbus training team will provide a customized training program designed to provide the State's employees with comprehensive knowledge of the Communicator software application and features. The session is designed to accommodate as many as 5 people with the full class running two (2) days. Interactive methods are supplemented by training materials such as CDs that support the educational needs of the participants.

- 1.1 Airbus will deliver a Training Agenda to State.
- 1.2 State will provide written acceptance of Training Agenda.
- 1.3 The State will provide an adequate facility for all onsite training events.
- 1.4 Airbus will travel to State's site to complete onsite Training.
- 1.5 Airbus will deliver Certificates of Training Completion.

2. Delivery Method – One-day, Web-Based, Interactive Training

Internet-based training is real-time, instructor-led training which covers all material necessary to optimize system performance and use of the Communicator. One web-based session (up to 10 participants/session) is available at no charge once per contract year.

3. Delivery Method - Pre-recorded Web-based Training Sessions

Computer-based training modules are located on the Airbus Support website at <http://support.AirbusDScommunications.com>. This self-paced training option is designed to provide System Administrators and/or End Users with an all-inclusive understanding of the Airbus Software and features, and is accessed through the Airbus Learning Management System for up to 12 months from time of approved registration.

The table below provides a summary of Airbus-provided Training Services:

Type	Delivery Method	Training Goal
Instructor-Led Class Training	Onsite	To provide State employees with comprehensive knowledge of the Communicator software application and features.
Web-Based Interactive Training	Remotely	To optimize system performance and use of the Communicator.
Pre-recorded web-based training	Remotely	This self-paced training option is designed to provide System Administrators and/or End Users with an all-inclusive understanding of the Airbus Software and features.

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR NXT HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT - PART 3
EXHIBIT L
TRAINING SERVICES

4. Key User Training Approach Activities

4.1 Identify State End Users

The Airbus Team shall lead the State in identifying and categorizing its end users:

User Category 1—Creators: Creator users have the ability to: view/edit personal contact information; create, view, modify and remove all groups assigned to his/her department; create, delete and modify his/her own scenarios and messages.

User Category 2—Roster Users: Roster users have the ability to: view/edit personal contact information

User Category 3—System Administrators: System Administrative Users have the ability to: view/ add, delete and/or edit all contact information; create, view, modify and remove all groups, messages and scenarios; assign security roles and password rules; reset passwords for all users.

User Category 4—Users: Users have the ability to: view/edit personal contact information; view, modify and remove groups assigned to his/her department; view, modify, remove, activate and stop scenarios assigned to his/her department.

4.2 Develop Training Plan

The Training Plan shall address the specific curriculum for each user category and provide support for the design, development, and deployment of training for each user category.

4.3 Develop Training Curriculum

Airbus shall develop a recommended training curriculum for the State of New Hampshire End Users.

4.4 Produce Training Materials and End-User Documentation

The Airbus Team shall lead the efforts to produce the training materials and to provide access to end-user Documentation.

4.5 Transfer Training Materials and End-User Documentation to the State

The Airbus Team shall provide training materials and End-User Documentation as project deliverables. Upon the State's request Airbus shall deliver updated training material to the State for the duration of the Contact.

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR NXT HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-094
AGREEMENT - PART 3
EXHIBIT M
RESERVED

RESERVED

**STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR NXT HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT - PART 3
EXHIBIT N
VENDOR PROPOSAL**

Airbus DS Communications, Inc. Proposal No. DIR50392, dated April 6, 2015, is attached (Attachment 3).

**STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR NXT HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049
AGREEMENT - PART 3
EXHIBIT O
SPECIAL EXHIBITS, ATTACHMENTS, AND CERTIFICATES**

Attached are:

1. Attachment 1- Department of Health and Human Services Exhibits D through J
2. Attachment 2-Contract Requirements
3. Attachment 3-Airbus DS Communications, Inc. Proposal No. DIR50392, dated July 6, 2015
4. Contractor's Certificate of Good Standing
5. Contractor's Certificate of Vote/Authority
6. Contractor's Certificate of Insurance

Contract 2015-049 Agreement – Part 3 Exhibit O-Certificates and Attachments

Initial and Date All Pages:

Airbus Initials AC

Date: 7-24-2015

**New Hampshire Department of Health and Human Services
Exhibit D**



CERTIFICATION REGARDING DRUG-FREE WORKPLACE REQUIREMENTS

The Contractor identified in Section 1.3 of the General Provisions agrees to comply with the provisions of Sections 5151-5160 of the Drug-Free Workplace Act of 1988 (Pub. L. 100-690, Title V, Subtitle D; 41 U.S.C. 701 et seq.), and further agrees to have the Contractor's representative, as identified in Sections 1.11 and 1.12 of the General Provisions execute the following Certification:

ALTERNATIVE I - FOR GRANTEES OTHER THAN INDIVIDUALS

**US DEPARTMENT OF HEALTH AND HUMAN SERVICES - CONTRACTORS
US DEPARTMENT OF EDUCATION - CONTRACTORS
US DEPARTMENT OF AGRICULTURE - CONTRACTORS**

This certification is required by the regulations implementing Sections 5151-5160 of the Drug-Free Workplace Act of 1988 (Pub. L. 100-690, Title V, Subtitle D; 41 U.S.C. 701 et seq.). The January 31, 1989 regulations were amended and published as Part II of the May 25, 1990 Federal Register (pages 21681-21691), and require certification by grantees (and by inference, sub-grantees and sub-contractors), prior to award, that they will maintain a drug-free workplace. Section 3017.630(c) of the regulation provides that a grantee (and by inference, sub-grantees and sub-contractors) that is a State may elect to make one certification to the Department in each federal fiscal year in lieu of certificates for each grant during the federal fiscal year covered by the certification. The certificate set out below is a material representation of fact upon which reliance is placed when the agency awards the grant. False certification or violation of the certification shall be grounds for suspension of payments, suspension or termination of grants, or government wide suspension or debarment. Contractors using this form should send it to:

Commissioner
NH Department of Health and Human Services
129 Pleasant Street,
Concord, NH 03301-6505

1. The grantee certifies that it will or will continue to provide a drug-free workplace by:
 - 1.1. Publishing a statement notifying employees that the unlawful manufacture, distribution, dispensing, possession or use of a controlled substance is prohibited in the grantee's workplace and specifying the actions that will be taken against employees for violation of such prohibition;
 - 1.2. Establishing an ongoing drug-free awareness program to inform employees about
 - 1.2.1. The dangers of drug abuse in the workplace;
 - 1.2.2. The grantee's policy of maintaining a drug-free workplace;
 - 1.2.3. Any available drug counseling, rehabilitation, and employee assistance programs; and
 - 1.2.4. The penalties that may be imposed upon employees for drug abuse violations occurring in the workplace;
 - 1.3. Making it a requirement that each employee to be engaged in the performance of the grant be given a copy of the statement required by paragraph (a);
 - 1.4. Notifying the employee in the statement required by paragraph (a) that, as a condition of employment under the grant, the employee will
 - 1.4.1. Abide by the terms of the statement; and
 - 1.4.2. Notify the employer in writing of his or her conviction for a violation of a criminal drug statute occurring in the workplace no later than five calendar days after such conviction;
 - 1.5. Notifying the agency in writing, within ten calendar days after receiving notice under subparagraph 1.4.2 from an employee or otherwise receiving actual notice of such conviction. Employers of convicted employees must provide notice, including position title, to every grant officer on whose grant activity the convicted employee was working, unless the Federal agency

**New Hampshire Department of Health and Human Services
Exhibit D**



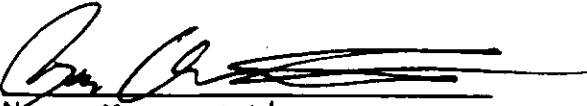
- has designated a central point for the receipt of such notices. Notice shall include the identification number(s) of each affected grant;
- 1.6. Taking one of the following actions, within 30 calendar days of receiving notice under subparagraph 1.4.2, with respect to any employee who is so convicted
 - 1.6.1. Taking appropriate personnel action against such an employee, up to and including termination, consistent with the requirements of the Rehabilitation Act of 1973, as amended; or
 - 1.6.2. Requiring such employee to participate satisfactorily in a drug abuse assistance or rehabilitation program approved for such purposes by a Federal, State, or local health, law enforcement, or other appropriate agency;
 - 1.7. Making a good faith effort to continue to maintain a drug-free workplace through implementation of paragraphs 1.1, 1.2, 1.3, 1.4, 1.5, and 1.6.
2. The grantee may insert in the space provided below the site(s) for the performance of work done in connection with the specific grant.

Place of Performance (street address, city, county, state, zip code) (list each location)

Check ☐ if there are workplaces on file that are not identified here.

Contractor Name:

7-21-2015
Date


Name: Ryan Christman
Title: Legal Counsel

New Hampshire Department of Health and Human Services
Exhibit E



CERTIFICATION REGARDING LOBBYING

The Contractor identified in Section 1.3 of the General Provisions agrees to comply with the provisions of Section 319 of Public Law 101-121, Government wide Guidance for New Restrictions on Lobbying, and 31 U.S.C. 1352, and further agrees to have the Contractor's representative, as identified in Sections 1.11 and 1.12 of the General Provisions execute the following Certification:

US DEPARTMENT OF HEALTH AND HUMAN SERVICES - CONTRACTORS
US DEPARTMENT OF EDUCATION - CONTRACTORS
US DEPARTMENT OF AGRICULTURE - CONTRACTORS

Programs (indicate applicable program covered):

- *Temporary Assistance to Needy Families under Title IV-A
- *Child Support Enforcement Program under Title IV-D
- *Social Services Block Grant Program under Title XX
- *Medicaid Program under Title XIX
- *Community Services Block Grant under Title VI
- *Child Care Development Block Grant under Title IV

The undersigned certifies, to the best of his or her knowledge and belief, that:

1. No Federal appropriated funds have been paid or will be paid by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any Federal contract, continuation, renewal, amendment, or modification of any Federal contract, grant, loan, or cooperative agreement (and by specific mention sub-grantee or sub-contractor).
2. If any funds other than Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this Federal contract, grant, loan, or cooperative agreement (and by specific mention sub-grantee or sub-contractor), the undersigned shall complete and submit Standard Form LLL, (Disclosure Form to Report Lobbying, in accordance with its instructions, attached and identified as Standard Exhibit E-I.)
3. The undersigned shall require that the language of this certification be included in the award document for sub-awards at all tiers (including subcontracts, sub-grants, and contracts under grants, loans, and cooperative agreements) and that all sub-recipients shall certify and disclose accordingly.

This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed by Section 1352, Title 31, U.S. Code. Any person who fails to file the required certification shall be subject to a civil penalty of not less than \$10,000 and not more than \$100,000 for each such failure.

Contractor Name:

7-21-2015
Date


Name: Ryan Christensen
Title: Legal Counsel

Exhibit E - Certification Regarding Lobbying

Contractor Initials RC

New Hampshire Department of Health and Human Services
Exhibit F



**CERTIFICATION REGARDING DEBARMENT, SUSPENSION
AND OTHER RESPONSIBILITY MATTERS**

The Contractor identified in Section 1.3 of the General Provisions agrees to comply with the provisions of Executive Office of the President, Executive Order 12549 and 45 CFR Part 76 regarding Debarment, Suspension, and Other Responsibility Matters, and further agrees to have the Contractor's representative, as identified in Sections 1.11 and 1.12 of the General Provisions execute the following Certification:

INSTRUCTIONS FOR CERTIFICATION

1. By signing and submitting this proposal (contract), the prospective primary participant is providing the certification set out below.
2. The inability of a person to provide the certification required below will not necessarily result in denial of participation in this covered transaction. If necessary, the prospective participant shall submit an explanation of why it cannot provide the certification. The certification or explanation will be considered in connection with the NH Department of Health and Human Services' (DHHS) determination whether to enter into this transaction. However, failure of the prospective primary participant to furnish a certification or an explanation shall disqualify such person from participation in this transaction.
3. The certification in this clause is a material representation of fact upon which reliance was placed when DHHS determined to enter into this transaction. If it is later determined that the prospective primary participant knowingly rendered an erroneous certification, in addition to other remedies available to the Federal Government, DHHS may terminate this transaction for cause or default.
4. The prospective primary participant shall provide immediate written notice to the DHHS agency to whom this proposal (contract) is submitted if at any time the prospective primary participant learns that its certification was erroneous when submitted or has become erroneous by reason of changed circumstances.
5. The terms "covered transaction," "debarred," "suspended," "ineligible," "lower tier covered transaction," "participant," "person," "primary covered transaction," "principal," "proposal," and "voluntarily excluded," as used in this clause, have the meanings set out in the Definitions and Coverage sections of the rules implementing Executive Order 12549: 45 CFR Part 76. See the attached definitions.
6. The prospective primary participant agrees by submitting this proposal (contract) that, should the proposed covered transaction be entered into, it shall not knowingly enter into any lower tier covered transaction with a person who is debarred, suspended, declared ineligible, or voluntarily excluded from participation in this covered transaction, unless authorized by DHHS.
7. The prospective primary participant further agrees by submitting this proposal that it will include the clause titled "Certification Regarding Debarment, Suspension, Ineligibility and Voluntary Exclusion - Lower Tier Covered Transactions," provided by DHHS, without modification, in all lower tier covered transactions and in all solicitations for lower tier covered transactions.
8. A participant in a covered transaction may rely upon a certification of a prospective participant in a lower tier covered transaction that it is not debarred, suspended, ineligible, or involuntarily excluded from the covered transaction, unless it knows that the certification is erroneous. A participant may decide the method and frequency by which it determines the eligibility of its principals. Each participant may, but is not required to, check the Nonprocurement List (of excluded parties).
9. Nothing contained in the foregoing shall be construed to require establishment of a system of records in order to render in good faith the certification required by this clause. The knowledge and

New Hampshire Department of Health and Human Services
Exhibit F



information of a participant is not required to exceed that which is normally possessed by a prudent person in the ordinary course of business dealings.

10. Except for transactions authorized under paragraph 6 of these instructions, if a participant in a covered transaction knowingly enters into a lower tier covered transaction with a person who is suspended, debarred, ineligible, or voluntarily excluded from participation in this transaction, in addition to other remedies available to the Federal government, DHHS may terminate this transaction for cause or default.

PRIMARY COVERED TRANSACTIONS


11. The prospective primary participant certifies to the best of its knowledge and belief, that it and its principals:
- 11.1. are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by any Federal department or agency;
 - 11.2. have not within a three-year period preceding this proposal (contract) been convicted of or had a civil judgment rendered against them for commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (Federal, State or local) transaction or a contract under a public transaction; violation of Federal or State antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property;
 - 11.3. are not presently indicted for otherwise criminally or civilly charged by a governmental entity (Federal, State or local) with commission of any of the offenses enumerated in paragraph (I)(b) of this certification; and
 - 11.4. have not within a three-year period preceding this application/proposal had one or more public transactions (Federal, State or local) terminated for cause or default.
12. Where the prospective primary participant is unable to certify to any of the statements in this certification, such prospective participant shall attach an explanation to this proposal (contract).

LOWER TIER COVERED TRANSACTIONS

13. By signing and submitting this lower tier proposal (contract), the prospective lower tier participant, as defined in 45 CFR Part 76, certifies to the best of its knowledge and belief that it and its principals:
- 13.1. are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction by any federal department or agency.
 - 13.2. where the prospective lower tier participant is unable to certify to any of the above, such prospective participant shall attach an explanation to this proposal (contract).
14. The prospective lower tier participant further agrees by submitting this proposal (contract) that it will include this clause entitled "Certification Regarding Debarment, Suspension, Ineligibility, and Voluntary Exclusion - Lower Tier Covered Transactions," without modification in all lower tier covered transactions and in all solicitations for lower tier covered transactions.

Contractor Name:

7-11-2015
Date


Name: Ryan Christensen
Title: Legal Counsel

New Hampshire Department of Health and Human Services
Exhibit G



**CERTIFICATION OF COMPLIANCE WITH REQUIREMENTS PERTAINING TO
FEDERAL NONDISCRIMINATION, EQUAL TREATMENT OF FAITH-BASED ORGANIZATIONS AND
WHISTLEBLOWER PROTECTIONS**

The Contractor identified in Section 1.3 of the General Provisions agrees by signature of the Contractor's representative as identified in Sections 1.11 and 1.12 of the General Provisions, to execute the following certification:

Contractor will comply, and will require any subgrantees or subcontractors to comply, with any applicable federal nondiscrimination requirements, which may include:

- the Omnibus Crime Control and Safe Streets Act of 1968 (42 U.S.C. Section 3789d) which prohibits recipients of federal funding under this statute from discriminating, either in employment practices or in the delivery of services or benefits, on the basis of race, color, religion, national origin, and sex. The Act requires certain recipients to produce an Equal Employment Opportunity Plan;
- the Juvenile Justice Delinquency Prevention Act of 2002 (42 U.S.C. Section 5672(b)) which adopts by reference, the civil rights obligations of the Safe Streets Act. Recipients of federal funding under this statute are prohibited from discriminating, either in employment practices or in the delivery of services or benefits, on the basis of race, color, religion, national origin, and sex. The Act includes Equal Employment Opportunity Plan requirements;
- the Civil Rights Act of 1964 (42 U.S.C. Section 2000d, which prohibits recipients of federal financial assistance from discriminating on the basis of race, color, or national origin in any program or activity);
- the Rehabilitation Act of 1973 (29 U.S.C. Section 794), which prohibits recipients of Federal financial assistance from discriminating on the basis of disability, in regard to employment and the delivery of services or benefits, in any program or activity;
- the Americans with Disabilities Act of 1990 (42 U.S.C. Sections 12131-34), which prohibits discrimination and ensures equal opportunity for persons with disabilities in employment, State and local government services, public accommodations, commercial facilities, and transportation;
- the Education Amendments of 1972 (20 U.S.C. Sections 1681, 1683, 1685-86), which prohibits discrimination on the basis of sex in federally assisted education programs;
- the Age Discrimination Act of 1975 (42 U.S.C. Sections 6106-07), which prohibits discrimination on the basis of age in programs or activities receiving Federal financial assistance. It does not include employment discrimination;
- 28 C.F.R. pt. 31 (U.S. Department of Justice Regulations – OJJDP Grant Programs); 28 C.F.R. pt. 42 (U.S. Department of Justice Regulations – Nondiscrimination; Equal Employment Opportunity; Policies and Procedures); Executive Order No. 13279 (equal protection of the laws for faith-based and community organizations); Executive Order No. 13559, which provide fundamental principles and policy-making criteria for partnerships with faith-based and neighborhood organizations;
- 28 C.F.R. pt. 38 (U.S. Department of Justice Regulations – Equal Treatment for Faith-Based Organizations); and Whistleblower protections 41 U.S.C. §4712 and The National Defense Authorization Act (NDAA) for Fiscal Year 2013 (Pub. L. 112-239, enacted January 2, 2013) the Pilot Program for Enhancement of Contract Employee Whistleblower Protections, which protects employees against reprisal for certain whistle blowing activities in connection with federal grants and contracts.

The certificate set out below is a material representation of fact upon which reliance is placed when the agency awards the grant. False certification or violation of the certification shall be grounds for suspension of payments, suspension or termination of grants, or government wide suspension or debarment.

Exhibit G

Contractor Initials

AC

Certification of Compliance with requirements pertaining to Federal Nondiscrimination, Equal Treatment of Faith-Based Organizations and Whistleblower protections

6/27/14

Rev. 10/21/14

Page 1 of 2

Page 6 of 16

Date 7-21-2015

**New Hampshire Department of Health and Human Services
Exhibit G**



In the event a Federal or State court or Federal or State administrative agency makes a finding of discrimination after a due process hearing on the grounds of race, color, religion, national origin, or sex against a recipient of funds, the recipient will forward a copy of the finding to the Office for Civil Rights, to the applicable contracting agency or division within the Department of Health and Human Services, and to the Department of Health and Human Services Office of the Ombudsman.

The Contractor identified in Section 1.3 of the General Provisions agrees by signature of the Contractor's representative as identified in Sections 1.11 and 1.12 of the General Provisions, to execute the following certification:

1. By signing and submitting this proposal (contract) the Contractor agrees to comply with the provisions indicated above.

Contractor Name:

7-21-2015
Date



Name: Ryan Christensen
Title: Legal Counsel

Exhibit G

Contractor Initials AC

Certification of Compliance with requirements pertaining to Federal Nondiscrimination, Equal Treatment of Faith-Based Organizations and Whistleblower protections

New Hampshire Department of Health and Human Services
Exhibit H



CERTIFICATION REGARDING ENVIRONMENTAL TOBACCO SMOKE


Public Law 103-227, Part C - Environmental Tobacco Smoke, also known as the Pro-Children Act of 1994 (Act), requires that smoking not be permitted in any portion of any indoor facility owned or leased or contracted for by an entity and used routinely or regularly for the provision of health, day care, education, or library services to children under the age of 18, if the services are funded by Federal programs either directly or through State or local governments, by Federal grant, contract, loan, or loan guarantee. The law does not apply to children's services provided in private residences, facilities funded solely by Medicare or Medicaid funds, and portions of facilities used for inpatient drug or alcohol treatment. Failure to comply with the provisions of the law may result in the imposition of a civil monetary penalty of up to \$1000 per day and/or the imposition of an administrative compliance order on the responsible entity.

The Contractor identified in Section 1.3 of the General Provisions agrees, by signature of the Contractor's representative as identified in Section 1.11 and 1.12 of the General Provisions, to execute the following certification:

1. By signing and submitting this contract, the Contractor agrees to make reasonable efforts to comply with all applicable provisions of Public Law 103-227, Part C, known as the Pro-Children Act of 1994.

Contractor Name:

7-21-2015
Date


Name: Ryan Christensen
Title: Legal Counsel

NH Department of Health and Human Services

STANDARD EXHIBIT I

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT
BUSINESS ASSOCIATE AGREEMENT

Standard Exhibit I, Health Insurance Portability and Accountability Act Business Associate Agreement, does not apply to this agreement.

New Hampshire Department of Health and Human Services
Exhibit J



**CERTIFICATION REGARDING THE FEDERAL FUNDING ACCOUNTABILITY AND TRANSPARENCY
ACT (FFATA) COMPLIANCE**

The Federal Funding Accountability and Transparency Act (FFATA) requires prime awardees of individual Federal grants equal to or greater than \$25,000 and awarded on or after October 1, 2010, to report on data related to executive compensation and associated first-tier sub-grants of \$25,000 or more. If the initial award is below \$25,000 but subsequent grant modifications result in a total award equal to or over \$25,000, the award is subject to the FFATA reporting requirements, as of the date of the award.

In accordance with 2 CFR Part 170 (Reporting Subaward and Executive Compensation Information), the Department of Health and Human Services (DHHS) must report the following information for any subaward or contract award subject to the FFATA reporting requirements:

1. Name of entity
2. Amount of award
3. Funding agency
4. NAICS code for contracts / CFDA program number for grants
5. Program source
6. Award title descriptive of the purpose of the funding action
7. Location of the entity
8. Principle place of performance
9. Unique identifier of the entity (DUNS #)
10. Total compensation and names of the top five executives if:
 - 10.1. More than 80% of annual gross revenues are from the Federal government, and those revenues are greater than \$25M annually and
 - 10.2. Compensation information is not already available through reporting to the SEC.


Prime grant recipients must submit FFATA required data by the end of the month, plus 30 days, in which the award or award amendment is made.

The Contractor identified in Section 1.3 of the General Provisions agrees to comply with the provisions of The Federal Funding Accountability and Transparency Act, Public Law 109-282 and Public Law 110-252, and 2 CFR Part 170 (Reporting Subaward and Executive Compensation Information), and further agrees to have the Contractor's representative, as identified in Sections 1.11 and 1.12 of the General Provisions execute the following Certification:

The below named Contractor agrees to provide needed information as outlined above to the NH Department of Health and Human Services and to comply with all applicable provisions of the Federal Financial Accountability and Transparency Act.

Contractor Name:

7-21-2015
Date


Name: Ryan Christensen
Title: Legal Counsel

New Hampshire Department of Health and Human Services
Exhibit J



FORM A

As the Contractor identified in Section 1.3 of the General Provisions, I certify that the responses to the below listed questions are true and accurate.

1. The DUNS number for your entity is: 046057446
2. In your business or organization's preceding completed fiscal year, did your business or organization receive (1) 80 percent or more of your annual gross revenue in U.S. federal contracts, subcontracts, loans, grants, sub-grants, and/or cooperative agreements; and (2) \$25,000,000 or more in annual gross revenues from U.S. federal contracts, subcontracts, loans, grants, subgrants, and/or cooperative agreements?

☒ NO ☐ YES

If the answer to #2 above is NO, stop here

If the answer to #2 above is YES, please answer the following:

3. Does the public have access to information about the compensation of the executives in your business or organization through periodic reports filed under section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C.78m(a), 78o(d)) or section 6104 of the Internal Revenue Code of 1986?

☐ NO ☐ YES

If the answer to #3 above is YES, stop here

If the answer to #3 above is NO, please answer the following:

4. The names and compensation of the five most highly compensated officers in your business or organization are as follows:

Name: _____	Amount: _____
Name: _____	Amount: _____
Name: _____	Amount: _____
Name: _____	Amount: _____
Name: _____	Amount: _____

AIRBUS DS COMMUNICATIONS

home of VESTA™

NH Department of Health & Human Services

Customer: Denise Krol

Date: 7/6/2015

Account Exec: Hope Baker
hope.baker@airbus-dscomm.com
(615) 435-4872

Proposal: DIR50392

(Quote is valid for 90 days)

Thank you for the opportunity for Airbus DS Communications to provide our industry renowned Notification Solutions and Services (NSS).

We are committed to providing our valued customers with the very best emergency notification technology. As part of this effort, we are pleased to announce the general availability of Version 4.4 for The Communicator!® NXT™ notification solution.

Our new release includes: "Blast Notification" MassCall access to 30,000 phone lines in our hosting center for large capacity call outs with lightning fast delivery, SAML Authentication (Single Sign On), Data Auditing & Change Logging, Two-Way SMS, Record Messages by Phone, compatibility with Microsoft Windows Server 2008 R2 SP1 64-bit Operating System, Web Browser compatibility (IE 7-11, Safari, Google Chrome, Mozilla Firefox, etc.) and much more (please see attachment).

Should you have any questions regarding your proposed Airbus DS Communications solution, please contact your NSS Account Executive at the information detailed above.

Solution Offered: Hosted The Communicator! NXT 4.4.2

Term: 5 Years (rate lock-in)

Includes:

- **Web-Based Application:** software accessible using a web browser (via Internet, LAN, or WAN)
- **Notify directly** from desktop or remotely by phone
- **List-based Notification:** contact groups of any size or type
- **Application easily fills positions** based on specific criteria such as skill, certification, and availability
- **User can modify** contacts, prepare messages, access results, easily managing communications from start to finish
- **Provides individuals** with situational details or instructions via phone (landline or cell), SMS Text, email and pagers
- **Two-way SMS Messaging**
- **Notification Methods:** mobile device, fax (optional), telephone, SMS Text, email, pager, overhead page
- **Record By Phone:** new voice message creation tool

- **Qualification Methods:** phone, email, SMS
- **Unlimited Emails** at no cost
- **Enhanced Browser Compatibility (version 4.4)** security Users can access The Communicator! NXT notification solution using their preferred web browser: Firefox®, Google Chrome™, Safari®, Microsoft® Internet Explorer® 7-11
- **Advanced Encryption Standard:** data integrity is always a topic of interest for database managers and system administrators alike. With this in mind, Airbus DS Communications has incorporated AES (256-bit) encryption to better protect your security information including passwords and PIN numbers.
- **SAML Authentication**
- **"Chat" with Technical Support directly from Communicator! NXT**
- **Improved Web Accessibility for the Disabled**
- **Up to 10 concurrent users**
- **Customize "Caller ID"** Displayed to Call Recipient by Company
- **Web/telephone Check-in** allows you to automatically validate the well-being of your personnel, ultimately maximizing employee accountability measures. Personnel provide their status by telephone or through a secure website, and reports provide check-in responses for follow-up action
- **40,000 Universal Minutes per year**- refresh yearly
- **Add-on Module:** choose two (2) from: API SDK, Blast Notification (MassCall), Survey, Conference Bridge/Call Transfer, Community Care (Calling Tree), or In-bound Bulletin Board (for descriptions, see Modules)
- **Custom Reports:** create your own reports, specifically designed by you
- **Auto Import** feature directs The Communicator! NXT to watch a designated directory or folder for a data file, which is automatically imported without human intervention based on a designated schedule/frequency
- **Hosted Backup:** a secondary redundant system provides near real-time backup of your primary system to a standby server located in our Mesa, AR hosting center. This option allows your operation to use an alternate server should your primary server be rendered unavailable or inoperative for any reason
- **EFax Service** (<http://www.efax.com>) Choose from EFax options below; add cost to total price
- **Annual Software Maintenance, and Support Plan**
- **24/7 multi-tier Technical Services Help Desk** made up of a team of full-time professionals, dedicated to providing the highest level of technical support by telephone, email and chat ("Chat" feature now available from NXT portal)
- **Free Software Updates/Upgrades** (within same product)
- **Eligibility** for all product migration and upgrade discounts
- **Training:** unlimited access to Computer-based Training modules (CBT's)
- **Training:** each year receive one live, Web-based training session for up to 10 people

AIRBUS DS COMMUNICATIONS

home of VESTA™

Cost Options

Contacts (based on 5 Yr Agreement)

9,000 Contacts: \$21,787 (annually)

Contacts (based on 30 day terms)

9,000 Contacts: \$26,000 (annually)

Additional Minutes/Units

10,000 Universal Calling and SMS Units (.10/unit)		\$1,000.00
25,000 Universal Calling and SMS Units (.09/unit)		\$2,250.00
50,000 Universal Calling and SMS Units (.08/unit)		\$4,000.00
100,000 Universal Calling and SMS Units (.06/unit)		\$6,000.00
250,000 Universal Calling and SMS Units (.055/unit)		\$13,750.00
500,000 Universal Calling and SMS Units (.05/unit)		\$25,000.00

EFAX Options (new pricing)

EFax Service w/1K pages/month (per year)	\$1,545.00
EFax Service w/3K pages/month (per year)	\$4,665.00
EFax Service w/5K pages/month (per year)	\$7,785.00
EFax Service w/7K pages/month (per year)	\$10,900.00
EFax Service w/10K pages/month (per year)	\$15,585.00

EFAX Options (old pricing; we will honor this pricing, if chosen)

EFax Service w/1K pages/month (per year)	\$1,750.00
EFax Service w/50K pages/month (per year)	\$7,350.00

NXT Training: On-site

Onsite NXT Training 5 participants:	\$4,200
On-site NXT training 10 participants:	\$6,200
On-site NXT training 15 participants:	\$7,950
On-site NXT training 20 participants:	\$7,200
On-site NXT training 30 participants:	\$10,200

NXT Training: In-house

NXT Training NSS (in-house) – one seat (1):	\$750
NXT Training - > two seats (per seat):	\$500

NXT Training: Web-based

NXT Web Training (up to 10 participants)	\$500
--	-------

Project Implementation

Comprehensive:	\$1,500
----------------	---------

Add-on Modules

NXT MassCall (per year)	\$2,500 (annually)
NXT Information Hotline (Bulletin Board Package)	\$2,995 (annually)
XML API, SDK in Hosting	\$4,995 (annually)
Transfer to Conferencing in Hosting	\$2,500 (annually)

Your requested modules; choose two @ no additional charge

Modules

Airbus DS Communications understands that every organization has unique communications needs, and has developed a variety of add-on's to complement your existing configuration. *Some options may have already been included in your plan, above.*

Additional Company

A Company enables you to completely segregate your organization's data into separate databases within your emergency notification solution. This ensures data integrity and provides security when other departments or agencies share the system, as they cannot view or modify information outside of their own Company.

API SDK (XML, SOAP and .NET API)

The Application Programming Interface (API) allows The Communicator! NXT to integrate with other technologies inside your organization (e.g., HR databases, overhead paging systems, BC/DR tools, etc.), further streamlining your critical communication processes. It also provides you the ability to configure the system in any language through the user interface (using double-byte support).

Auto Import

The Auto Import feature directs The Communicator! NXT to watch a designated directory or folder for a data file, which is automatically imported without human intervention based on a designated schedule/frequency.

Community Care (Calling Tree)

Community Care enables designated caregivers to feel confident knowing the individuals they are responsible for are being automatically checked on by telephone when unaccompanied. More importantly, if the person cannot be reached or indicates that he/she needs help, the caregiver is alerted of the situation or local authorities are notified to send someone to the residence.

Conference Bridge/Call Transfer

The Conference Bridge/Call Transfer option serves as a virtual meeting place, bringing key individuals together by telephone. This option can be set up to transfer call recipients to a conference bridge, live operator, help desk or other designated telephone line. It can also be used to transfer a call recipient into The Communicator! NXT to activate other scenarios.

DataSync Back-up

Using SQL Server™ backup and restore technology, DataSync Back-up provides near real-time back-up of The Communicator! NXT to a standby server located in Airbus DS Communications Hosting Center. This option creates a redundant system, allowing your operation to use an alternate server should your primary server be rendered unavailable or inoperable for any reason.

Desktop Alerting

Airbus DS Communications provides desktop alerting applications, which instantly disseminate messages to the screens of any networked PC or laptop. Depending on your needs, audible and/or visual alerts take precedence over all other open applications, ensuring the notification is received.

Inbound Bulletin Board

The Inbound Bulletin Board is used to deliver status updates or general information to incoming callers (e.g., residents, community groups, employees, etc.). It can be used to provide emergency or everyday information, saving time and resources from answering routine informational calls.

GeoCast Web Back-up

Airbus DS Communications GeoCast Web Back-up provides back-up of GeoCast Web to a standby server located in the company's Hosting Center. This option creates redundancy of your maps, allowing your operation to use an alternate server should your primary server be rendered unavailable or inoperable for any reason.

Self-Registration Portal (SRP)

The SRP is a customizable, highly secure and easy-to-access web tool that allows people to sign up to receive notifications. Once implemented, the option to "click to register" appears on your website or intranet, quickly linking individuals to the SRP's URL. Here, they can complete a short web form, supplying their physical/email addresses and phone numbers. In addition, they can opt in their SMS device to receive text messages, or even select to receive emergency and/or routine messages.

Survey

The Survey module allows you to compose any number of questions for delivery via phone and/or email. It can be used to collect information pertaining to a variety of events, including pandemics, hurricanes, service outages and more. The Survey module also allows individuals to provide feedback about their well-being, enabling you to know if they are safe and okay. Responses are viewed in real-time reports, available in detail and summary formats.

Web/Telephone Check-In

Web/Telephone Check-In allows you to automatically validate the well-being of your personnel, ultimately maximizing employee accountability measures. Personnel provide their status by telephone or through a secure website, and reports provide check-in responses for follow-up action.

NXT Blast Notification (MassCall)

New Activation option that provides a simultaneous message broadcast to all selected devices (instead of using a device sequence). Activation logic is optimized for rapid message delivery. Utilizes the MassCall service (30,000 phone lines) for fast delivery of telephone messages. Available as an add-on service for all Hosted and On-Premise customers using The Communicator!® NXT™ version 4.4.2

Installation

Airbus DS Communications provides a variety of resources to assist you in the successful implementation of your solution. Our Project Management services streamline communications and maximize efforts emergency of notification system deployments. A Project Manager will serve as a single point of contact and primary project facilitator for all related issues during the implementation period through solution acceptance. Airbus DS Communications uses a phased approach to project implementation.

Phase I – Planning

Phase I is the period of time which the project is formally launched, the project design is finalized, a Project Plan is created and resources are scheduled. The Project Manager coordinates Phase I activities with the customer to ensure the project scope has been assessed, and that all deliverables have been integrated into a comprehensive Master Project Schedule that will be attached to the Project Plan. The Project Plan will be the control document for deliverables for the implementation as well as other critical dates or milestones that are integral to the project. Critical activities within Phase I include:

Project Launch Call

- Scheduled as soon as possible following receipt of a sales order.
- Process owners are identified
- Key project milestones and objectives are introduced and discussed.
- Review the overall project "As Purchased" design.
- First review of the draft Project Plan.

Design Review Meeting

- Usually accomplished within 15 days of the project launch.
- Detailed Review of the "As Purchased" system design.
- Project Plan Approval

Resources will be scheduled and communicated to the team members via the Master Project Schedule. The Master Schedule will be drafted and forwarded to team members for review and comment. This "first pass" schedule will be used to present the initial deployment schedule. Once all feedback and changes have been received and integrated into the schedule, the Master Schedule will be published by the Project Manager. Once published, the Master Schedule will only be changed as per appropriately submitted change requests.

The Planning Phase ends when:

- The Project Plan has been approved.
- System design is completed.

Phase II – Implementation

Phase II is the period of time in which system implementation and training take place. The project's implementation is accomplished to the degree that is possible without actually going "live". The Project Manager will coordinate the Phase II activities with the customer to minimize interference with other site activities, while ensuring that the implementation and training are completed as part of the Project Plan and the Master Project Schedule.

Installation

Implementation and training milestones and deliverables will be documented and managed via the Master Project Schedule. The Installation Responsibility Matrix delineates task level responsibilities for installation.

The Implementation Phase ends when:

- Hosting set-up is complete.
- Training has been completed to the degree agreed upon during the Project Planning Process.
- Testing is complete.

Phase III – Cutover Phase

The Cutover phase defines any deliverables required in the Implementation Phase, but not satisfied. If any such issues exist, the system will be placed in a locked down state. Once these issues are identified and agreed upon, the Project Manager will facilitate the completion of those items and services. Once all items have been completed, the Project and Software Acceptance is signed and the system will be unlocked and turned over to the customer.

Phase IV – Post Cut and Support

The Post Cut and Support Phase shall occur when the Project and Software Acceptance has been signed. Its purpose is to ensure immediate technical support to the customer if necessary. Any additional training or other services purchased, but not accomplished during the Implementation Phase, will be addressed in this Phase. In this phase, your Project Manager will transition the project to Technical Services. This will end the project manager's involvement on this project.

Snapshot

This is a basic overview/snapshot of the steps taken for a smooth transition for an on-premise to a hosted solution. These steps only apply to an NXT 4.2.1 to NXT 4.4 Conversion.

- Get NXT info from Customer.
- Submit requests to Infrastructure.
- Set up an agreed time for Cut-Over and Migrate Database and Reports (if desired)

Pre-Upgrade Backups:

- Run DB Snapshot
- Backup Call Flows
- Backup Import Files
- Backup Pager Scripts
- Backup Databases
- Create listing of Company Maintenance Settings
- Move all backups to FTP Site

Data Migration:

- Data freeze
- Get snapshot of current database
- Upgrade to v4.4

- Setup Paging/SMS
- Test Company to ensure devices working
- Add Company to DataSync
- Remove scheduled activation scenario settings
- Get snapshot of upgraded database

Test Primary Server:

- Compare Snapshot of data for data integrity
- Test Scenarios - Existing and New - Users will receive Activation Reports
- Test Messages - Existing and New
- Test Groups - Existing and New
- Check Security Users
- Check Scenario and Group Security Users
- Test Paging/SMS
- Test Email and Email Qualification
- Test Call Transfer (if applicable)

Primary System Acceptance:

- Finalize customer configurations
- Coordinate training dates (if applicable)

4.4 Backup System:

- Set up DataSync on backup

Move DataSync From Onsite Backup to v4.4 Backup:

- Infrastructure request to move existing backup URL and phone numbers to v4.4
- Complete project documentation
- Send URL, Login, and system access information to customer
- Stop DataSync from on-premise server

v4.4 Primary & Backup Server In Production.

Technical Services Center - Support Plan for Hosted Service

Airbus DS Communications, Inc. ("Airbus DS Communications") offers Airbus DS Communications Software support to purchasers ("Licensee" or "Customer") of its application Software, in accordance with the terms and conditions of this Technical Services Center Support Plan ("Support Plan"), which is made a part of and incorporated by reference into the Service Agreement ("Agreement") entered into by Customer and Airbus DS Communications. Defined terms as set forth in the Agreement shall have the same meaning in this Support Plan.

Conditions of the Support Plan

In order to keep the Support Plan active, the Customer is required to: Pay all applicable Service Agreement Fees; and Comply with all terms and conditions of this Support Plan and the Service Agreement.

Definitions

Response Time is the period of time that it takes the TSC to call back the Customer when a voice mail has been left or to provide an update on the call ticket. Response times are only implemented when the call is not resolved on the first call. Response Time does not mean Resolution Time. Resolution Time is the period of time it takes to solve a problem. The resolution time is different for each situation and cannot be determined until the appropriate TSC personnel have evaluated the problem and is able to determine an approximate resolution time.

TSC – Technical Services Center

TSS – Technical Services Specialist

TSA – Technical Services Analyst

Term of the Software Support Plan

The term of the Support Plan will commence with the Effective Date of the Service Agreement and will continue through the Initial Term and any Renewal Terms.

Support Services Provided

Supported Products

The TSC will only support Software approved and installed by Airbus DS Communications. The TSC will not resolve requests associated with software other than that provided by Airbus DS Communications; the requests will, however, be logged into the database. Pursuant to this Support Plan, Airbus DS Communications, as coordinated by its Technical Service Center, will provide issue resolution and updates to supported Software as further described below.

Hours of Operation

- Normal Business Hours (NBH): Monday through Friday, excluding holidays, from 8:00AM to 5:00PM, Central Time.
- After hours Emergency support only - see Call Levels

Services Provided

Issue Resolution

The TSC works with Customers to resolve issues related to supported Software that does not perform materially in accordance with the then current Documentation for such Software. This service is designed to support the Customer's system administrator technician who is adequately trained in the product about which they are calling and listed as an approved Customer Contact with Airbus DS Communications' TSC. To be adequately trained the Customer's system administrator technician must have received training directly through a Airbus DS Communications training program or have been trained by a Customer system administrator that has received training directly through Airbus DS Communications. A trained Customer's system administrator is responsible for attempting to troubleshoot issues prior to calling TSC. If the Customer's system administrator is not adequately trained, based on the description above, in the product about which he or she is calling, and thus not listed as an approved Customer Contact, Airbus DS Communications TSC personnel will attempt to contact an approved Customer contact for problem resolution.

For security purposes, only Customer contacts that are listed with TSC will receive support unless a listed contact provides approval to do so. In the event of an emergency TSC may make a special allowance if TSC personnel are unable to reach one of the listed contacts for verification.

The TSC will maintain a database of all calls received from the Customer, the steps taken to resolve and the resolution. The database will show dates when a call was received and dates of all contacts related to call.

TSC will work with the Customer to identify errors or defects in the Software, and if the TSC is unable to confirm that such error or defect exists through independent testing, it will then escalate the issue to Airbus DS Communications' R&D Department. The TSC will remain as the Customer contact and will work with the R&D Department to provide updated information to the Customer through resolution of the issue.

Contacting the Airbus DS Communications Technical Services Center

During Normal Business Hours: Customers may call 615.794.2307. If all TSC personnel are busy assisting other customers, the call will go to voice mail. If the caller is experiencing an emergency (see Call Levels below) they may hit 00 for the operator and a TSC manager will be paged to assist. If the call is not an emergency (as defined below), the caller should leave a message with their name, company name and ID, telephone number and a brief description of the reason for the call. Messages are checked frequently and calls are returned in the order in which they are received, but always within four (4) hours.

After Hours Emergency: If the Customer is experiencing an emergency (as defined below) they should call the TSC at 615.794.2307. The call will be routed to an answering service where the Customer should leave a clear message with their name, company name and ID, telephone number and a brief description of the reason for the call. The on-call TSS will be paged and will return the call within 15 minutes of receipt of the page.

E-mail Requests: The TSC will respond to e-mail requests within eight (8) business hours. Note: Emergency or very important requests should always be phoned into the TSC. E-mail can sometimes be unreliable and the TSC has no control over the timely delivery of requests. E-mail service level commitments are based on the time the requests reach the TSC.

Support Plan Call Levels

Emergency Call- Immediate Response during NBH; within 15 minutes of page outside NBH

- System will not boot or complete hardware failure.*
- Server Applications will not start.
- Site is experiencing an actual emergency and the system will not send out notifications to one or more device types.
- Site initiates activation, attempts to stop it, and experiences difficulty doing so.
- *If it is determined the system failure is due to software or hardware loaded without coordination with Cassidian Communications or other acts induced by the Customer, resources will be allocated as available to assist but response time is not guaranteed.

Routine Call - 4 hour Response Time

- Reports are not functioning properly.
- Testing system and needs help making adjustments.
- Assistance with modifying roster members or groups.
- Assistance with speech recording done by Site.
- Assistance creating template scenarios.
- Services that require advanced scheduling
- Installation of software or hardware updates or addition.
- Modifications to the system to accommodate telephony changes.
- Airbus DS Communications provided speech recording.
- GIS Updates.

Call Procedures & Escalation

The Technical Service Center will maintain call ownership throughout the entire request process.

The TSC will address incoming calls as follows.

1. Capture the Request - The TSS/TSA will capture all requests by phone, e-mail, or voice mail and verify the right to service based on the Customer's name, support contract status and the approved software support list. If the request relates to unsupported software, the Customer will be notified. Otherwise, the analyst will continue with Step 2.
2. Log Request into the Database - The TSS/TSA will open a ticket in the call management system. Information included on the ticket will include the Customer's name, location, description of problem, severity of problem, and time of request and person reporting the issue.
3. Troubleshoot the Request - The TSS/TSA responsible for resolving the call will acknowledge the open ticket and work with the Customer to resolve the issue.
4. Escalate to Second Level - The TSS will escalate the request to second level support when the first contact is unable to make progress in the resolution of the issue in a timely manner.
5. Log Resolution into the Database - The TSS/TSA will log the resolutions to requests in the call management database
6. Verifies Customer Satisfaction - The TSS/TSA will follow up and verify that the Customer is satisfied with the resolution.
7. Close the Request or Ticket - All tickets will be closed after the Customer satisfaction has been verified.

Services that require advanced scheduling

- Installation of software or hardware updates or addition.
- Modifications to the system to accommodate telephony changes.
- Cassidian Communications provided speech recording.
- GIS Updates.

Customer Responsibilities

- The Customer Site should have at least one system administrator that has attended Airbus DS Communications training, either at the Customer Site or at the Airbus DS Communications University. The Customer shall provide the administrator's contact information to Airbus DS Communications.
- Customer will schedule install of all updates in a timely manner
- Customer will work with TSC staff to maintain an accurate database of contact names.
- Customer will respond to requests for information in a timely manner.
- Payment of all service fees when due.
- Support Limitations

Airbus DS Communications' support obligations hereunder will not apply to any Airbus DS Communications supported application Software if correction of an error, adjustment, repair, or parts replacement is required because of:

- Damage or destruction caused by natural or man-made acts or disasters
- The operation of the software in a manner other than that currently specified by Airbus DS Communications.
- The failure of the Customer to provide suitable qualified and adequately trained operating and maintenance staff.

Further, support described herein does not include cosmetic repairs, making accessory changes or adding additional devices or software applications.

Software Updates

Airbus DS Communications will provide application Software updates. Application Software updates are defined as minor enhancements to the already purchased product feature / functionality set. A product change is classified as minor, in the discretion of Airbus DS Communications, based upon the impact of the change to the core functionality of the product. Notice of all Software updates available during the term of the Support Plan will be posted under the "latest Updates and Patches" section for each product on the Airbus DS Communications Support Website located at <http://support.AirbusDScommunications.com/> (login required). Application Software program updates will roll into the existing Support Plan, thereby not extending the term of the Support Plan. Any change in the two numbers following the decimal point within the product version number constitutes an application software program update (for example a change from product version 1.10 to 1.20 or 2.11 to 2.12, or 3.20 to 3.30, etc. will represent an application software program update).

Other Services

Other services not specifically identified as being included in this Support Plan, including but not limited to training, implementation services, and custom development, are not included.

Airbus DS Communications University

Airbus DS Communications offers a variety of training options, covering all topics necessary for optimum system performance and meeting any scheduling need

- **In-house:** In this two- and a half-day course held at Airbus DS Communications' Franklin, Tennessee, location, users can comfortably share ideas and network, exploring best practices for utilizing the technology within their operations. These comprehensive courses typically run Tuesday through Wednesday, 8:30 a.m. to 4 p.m. CST. Instruction covers all material necessary for optimum system performance and usage of this solution. Along with this learning experience, you will have the opportunity to meet members of the Airbus DS Communications team, as well as other system users, in a relaxed, yet highly informative setting.
- **On-site:** Clients can elect to have an experienced member of the training team come to your location, providing flexibility for multiple teams/shifts to take part and accommodating the most demanding of schedules. A truly customized training program, this option is designed to provide participants with comprehensive knowledge of The Communicator! NXT software application and their related feature sets. The session is designed to accommodate as many as 15 people, with the full class running up to two days. Interactive methodology, supplemented by training materials via CDs, support the educational needs of students and invoke theory in contingency-related communications
- **Web-based:** This option enables you to take part in real-time, instructor-led training specific to your organization and needs. Web training. Instruction covers all material necessary for optimum system performance and usage of The Communicator! NXT and GeoCast Web. Along with this learning experience, you will also become familiar with the Airbus DS Communications team and other system users, making it a relaxed, yet informative, setting for everyone to enjoy.
- **Pre-recorded Training Sessions:** Computer-based Training modules, at your convenience are located on our Support website at <http://support.AirbusDScommunications.com/>. This self-paced training option is designed to provide System Administrators and/or End Users with an all-inclusive understanding of the Airbus DS Communications solution software and feature sets, and is accessed through our Learning Management System for up to 12 months from time of approved registration (while currently under Support contract).

AIRBUS DS
COMMUNICATIONS

home of VESTA

Hosting Center Policies

Please see attachment "Hosting Center Policies" for more information on security, testing, maintenance, etc.

Service Agreement

This Service Agreement ("Agreement") is made and entered into this _____ day of _____, _____ ("Effective Date") by and between Airbus DS Communications, Inc., a California corporation ("Airbus DS Communications"), located at 42505 Rio Nedo, Temecula, CA 92590, or its authorized reseller, and NH Department of Health & Human Services ("Customer"), located at 29 Hazen Drive, Concord, NH 03301. Both Airbus DS Communications and Customer may alternatively be referred to as a "Party" and collectively as the "Parties".

1. Definitions.

1.1 "Content" means the audio and visual information, Documentation, Software, products and services contained or made available to Customer in the course of using the Service.

1.2 "Customer Data" means any data, information or material that Customer submits to the Service in the course of using the Service.

1.3 "Documentation" means on-line material provided by Airbus DS Communications or its authorized reseller to assist Customer in the use of the Service.

1.4 "Initial Service Term" means the period of time commencing on the online date for Services as set forth in the Customer Proposal DIR50392 ("Proposal") attached hereto and incorporated herein as Exhibit A.

1.5 "Airbus DS Communications Technology" means the Airbus DS Communications provided technology (including but not limited to Documentation, Software, hardware, equipment, products, processes, algorithms, user interfaces, know-how, techniques, designs, and other tangible or intangible technical material or information) made available to Customer by Airbus DS Communications in providing the Service.

1.6 "Software" means the application software programs and any updates, modifications and corrections thereto to which Airbus DS Communications has granted access to Customer as part of the Service hereunder.

1.7 "Service" means the emergency notification system accessible via the Internet and all associated applications and modules identified in the Proposal and purchased by Customer and all ancillary online or offline products and services provided to Customer by Airbus DS Communications hereafter.

1.8 "User" shall refer to Customer's employees, representatives, consultants, contractors or agents who are authorized to use the Service and have been supplied with user identifications and passwords by Customer.

2. Payment and Taxes.

2.1 **Customer's Purchase.** In consideration of the fees described herein, Airbus DS Communications or its authorized reseller shall provide Customer with access to the Service as described herein and as governed by the terms and conditions of this Agreement, accepted Proposal, and incorporated documents. Additional services may be added by the parties throughout the term of this Agreement through a subsequent proposal issued by Airbus DS Communications, which may be accepted through Customer purchase order and shall be governed by the terms and conditions set forth under this Agreement.

2.2 **Fees of Service.** For the Initial Service Term, Customer will pay Airbus DS Communications or its authorized reseller the amount set forth in the Proposal. Payment shall be made within thirty (30) days from the date of the invoice. License rights granted hereunder and Services shall automatically renew annually unless terminated by Customer's written notice to Airbus DS Communications or its authorized reseller not less than ninety (90) days prior to the expiration of the then in effect term. Airbus DS Communications or its authorized reseller shall invoice Customer for the renewal term sixty (60) calendar days prior to the then in effect term. Payment on the renewal invoice shall be due on or before the expiration of the current term.

2.3 **Calling Minutes / SMS Messages.** See Proposal.

2.4 **Taxes.** Customer will pay all taxes based on this Agreement or any product or services related thereto, excluding taxes based on Airbus DS Communications' income, but including personal property taxes, if any. All

Service Agreement

shipping and insurance charges for products shipped between Airbus DS Communications and Customer will be paid by Customer.

2.5 Late Charges. In addition to any other remedy available to Airbus DS Communications, for a late payment by Customer, Customer shall pay a charge of 1.5% per month, or the maximum percentage permitted by applicable law, whichever is less, on any amount not paid when due.

3. License, Access and Use of the Service.

3.1 License: Airbus DS Communications hereby grants Customer a non-exclusive, non-transferable, worldwide right to use the Service, solely for Customer's internal business purposes, subject to the terms and conditions of this Agreement. All rights not expressly granted to Customer are reserved by Airbus DS Communications and its licensors.

3.2 Access: Customer and Airbus DS Communications shall agree upon, prior to Customer's use of the Service, the offices and Users authorized to access the Service and such Users shall be identified in writing in advance by Customer. Customer may modify the Users of the Service by providing advance written notice to Airbus DS Communications. Customer may authorize access for the number of simultaneous, concurrent Users of the Service at any given time. Passwords provided for Service access may be used only by authorized personnel. Neither Customer nor its authorized personnel shall divulge, sublicense, assign or transfer to any third party passwords established for access to the Service. Customer shall be responsible for the confidentiality and security of its User identifications and passwords.

3.3 Customer Responsibilities: Customer is responsible for all activity occurring in its User accounts and shall abide by all applicable local, state, national and foreign law, treaties and regulations in connection with Customer's use of the Service, including but not limited to data privacy, security, international communications and the transmission of technical or personal data. Customer shall: (i) Prevent unauthorized access to the Service and notify Airbus DS Communications immediately of any unauthorized use of any password or account or any other known or suspected breach of security; (ii) report to Airbus DS Communications immediately and use reasonable efforts to stop immediately any copying or distribution of Content that is known or suspected by Customer; and (iii) ensure that use of the Service by all of Customer's Users is in compliance with this Agreement.

3.4 Restrictions: Customer shall not (i) license, sublicense, sell, resell, transfer, assign, distribute or otherwise commercially exploit or make available to any third party the Service or the Content in any way; (ii) modify or make derivative works based upon the Service or the Content; (iii) create Internet "links" to the Service or "frame" or "mirror" any Content on any other server or wireless or Internet-based device; (iv) send spam or otherwise duplicative or unsolicited messages in violation of applicable law; (v) send or store infringing, obscene, threatening, libelous, or otherwise unlawful or tortious material, including material harmful to children or violative of third party privacy rights; (vi) send or store material containing software viruses, worms, Trojan horses or other harmful computer code, files, scripts, agents or programs; (vii) interfere with or disrupt the integrity or performance of the Service or the data contained therein, including but not limited to Customer Data; (viii) attempt to gain unauthorized access to the Service or its related systems or networks; (ix) reverse engineer or access the Service in order to (a) build a competitive product or service, (b) build a product using similar ideas, features, functions or graphics of the Service, or (c) copy any ideas, features, functions or graphics of the Service.

4. Customer Data. Airbus DS Communications does not own any data, information or material that Customer submits to the Service in the course of using the Service ("Customer Data"). Customer shall have sole responsibility for the accuracy, quality, integrity, legality, reliability, appropriateness and intellectual property ownership or right to use of all Customer Data. Airbus DS Communications shall not be responsible or liable for the deletion, correction, destruction, damage loss or failure to store any Customer Data. Customer shall maintain a copy of all Customer Data. Customer is solely responsible for adherence to any privacy act or regulation regarding such Customer Data and Airbus DS Communications will have no responsibility with respect to the same. Regarding any self registration portal tool purchased or licensed by Customer through or with Airbus DS Communications, Customer shall assume all duties, obligations and compliance with any applicable law regarding its use, including but not limited to the gathering, storage and dissemination of such Customer Data. Customer shall also be solely

responsible for communicating any applicable notices or terms of use to its registrants. These duties and obligations are non-delegable by Customer to Airbus DS Communications.

5. Privacy and Security; Disclosure. Airbus DS Communications' Data Security and Encryption Policy and Hosting Center Policy are available upon Customer request. Airbus DS Communications reserves the right to modify these policies in its reasonable discretion from time to time. Note that because the Service is a hosted, online application, Airbus DS Communications may need to notify all Users of the Service of important announcements regarding the operation of the Service and will use Customer information for that purpose.

6. Training and Support Services

6.1 Training. Training, if purchased by Customer, will be reflected on the corresponding invoice.

6.2 Subject to the terms and conditions of this Agreement and provided that Customer pays all applicable fees related to the Service, Airbus DS Communications shall provide Customer with support described in this Agreement and as more particularly described in Airbus DS Communications' Technical Service Center Support Plan ("Support Plan") a copy of which may be viewed at <http://support.airbus-dscomm.com> and is incorporated herein by reference. Airbus DS Communications reserves the right to modify the terms and conditions of the Technical Service Center Support Plan at any time, effective upon posting of an updated version. Customer is responsible for regularly reviewing the TSC Support Plan. Continued use of the Service after any such changes shall constitute Customer's consent to such changes.

7. Warranty.

7.1 Warranty. Each Party represents and warrants that it has the legal power and authority to enter into this Agreement. Airbus DS Communications represents and warrants that it will provide the Service in a manner consistent with general industry standard reasonably applicable to the provision thereof and that the Services will perform substantially in accordance with the online Airbus DS Communications Documentation under normal use and circumstances. The Customer represents and warrants that it has not falsely identified itself or provided any false information to gain access to the Service.

7.1.1 During the Initial Service Term, Airbus DS Communications will provide such assistance as it deems reasonably necessary to cause the Airbus DS Communications Service to perform materially in accordance with the then current Documentation provided that Customer's use is in accordance with this Agreement and the Documentation.

7.1.2 Customer's Remedy: CUSTOMER'S EXCLUSIVE REMEDY, AND AIRBUS DS COMMUNICATIONS ENTIRE LIABILITY IN CONTRACT, TORT OR OTHERWISE FOR BREACH OF ANY OF THE ABOVE WARRANTIES WILL BE TO USE ITS COMMERCIALY REASONABLE EFFORTS TO PROVIDE A CORRECTION OR WORK AROUND FOR ANY MATERIAL NONCONFORMITY WHICH IS (i) REPORTED TO AIRBUS DS COMMUNICATIONS BY CUSTOMER WHILE AIRBUS DS COMMUNICATIONS IS OBLIGATED TO PERFORM SUPPORT SERVICES AND (ii) REPRODUCIBLE BY AIRBUS DS COMMUNICATIONS IN THE EXECUTION ENVIRONMENT.

7.2 Disclaimer of Warranties. THE EXPRESS WARRANTIES CONTAINED IN THIS AGREEMENT ARE EXCLUSIVE AND IN LIEU OF ALL OTHER REPRESENTATIONS AND WARRANTIES. AIRBUS DS COMMUNICATIONS DISCLAIMS ALL OTHER WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. AIRBUS DS COMMUNICATIONS DOES NOT WARRANT THAT THE SOFTWARE OR SERVICE IS ERROR-FREE OR WILL OPERATE WITHOUT INTERRUPTION.

IF THE AIRBUS DS COMMUNICATIONS SERVICE IS USED IN EMERGENCY SITUATIONS, THEN THE SERVICE IS INTENDED TO ONLY INCREASE THE NOTICE WHICH WILL BE GIVEN. THERE IS AND CAN NOT BE ANY GUARANTEE THAT ALL PERSONS INTENDED TO BE CONTACTED WILL BE CONTACTED. AIRBUS DS COMMUNICATIONS ACCEPTS NO RESPONSIBILITY FOR ANY FAILURE OF THE AIRBUS DS COMMUNICATIONS SERVICE TO CONTACT ANY PERSON OR PERSONS AND IS NOT

Service Agreement

RESPONSIBLE FOR ANY DAMAGE OR INJURY WHICH RESULTS FROM ANY FAILURE TO CONTACT ANYONE.

7.3 The warranties in this Section 7 will not apply to any defects or problems caused in whole or part by (i) defects in any equipment, (ii) failure of any portion of equipment to function in accordance with manufacturer's

specifications, (iii) modifications or enhancements made to the Service by anyone other than Airbus DS Communications, (iv) any software, hardware, firmware, peripheral or communication devices used with the Service not provided by or approved of in writing by Airbus DS Communications, (v) failure of Customer or any third party to follow Airbus DS Communications' most current instructions for proper use of the Service, (vi) negligence of Customer or any third party, or (vii) failure to install and use the updates, modifications and corrections provided by Airbus DS Communications. If Customer falls within any of the foregoing exceptions and requests Airbus DS Communications to provide support services for such defect or problem, Customer will pay Airbus DS Communications for such services at Airbus DS Communications' then current hourly rate.

7.4 **Intellectual Property, Trademark and Copyright.** Airbus DS Communications retains ownership of the Software and Service, any portions or copies thereof, and all rights therein. Airbus DS Communications reserves all rights not expressly granted to Customer. This Agreement does not grant Customer any rights in connection with any trademarks or service marks of Airbus DS Communications, its suppliers or licensors. All right, title, interest and copyrights in and to the Software, Service and Documentation and any copies thereof are owned by Airbus DS Communications, its suppliers or licensors. All title and intellectual property rights in and to the Content which may be accessed through use of the Service is the property of the respective Content owner and may be protected by applicable copyright or other intellectual property laws and treaties. This Agreement grants Customer no rights to use such Content.

8. **Limitation of Liability.** IN NO EVENT WILL AIRBUS DS COMMUNICATIONS BE LIABLE TO CUSTOMER FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR PUNITIVE DAMAGES, INCLUDING WITHOUT LIMITATION, LOSS OF DATA, LOSS OF PROFITS, LOSS OF BUSINESS INFORMATION, BUSINESS INTERRUPTION OR ANY OTHER PECUNIARY LOSS ARISING OUT OF THE USE OF OR INABILITY TO USE THE SERVICE OR SOFTWARE OR THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT SERVICES, ARISING OUT OF OR RELATED TO THIS AGREEMENT, EVEN IF AIRBUS DS COMMUNICATIONS HAS BEEN ADVISED OF, KNEW OF, OR SHOULD HAVE KNOWN OF THE POSSIBILITY OF SUCH DAMAGES. AIRBUS DS COMMUNICATIONS'S TOTAL LIABILITY TO CUSTOMER HEREUNDER, IF ANY, WILL IN NO EVENT EXCEED THE TOTAL AMOUNT PAID TO AIRBUS DS COMMUNICATIONS HEREUNDER IN THE TWELVE (12) MONTHS IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO THE CLAIM.

9. **Confidentiality.** A Party receiving Information (defined below) of the other will not disclose such Information other than to persons in its organization who have a need to know and who will be required to comply with this Section 9. The Party receiving Information will not use such Information for a purpose inconsistent with the terms of this Agreement. "Information" means the Software, Documentation and all information and intellectual property related thereto (including, but not limited to all databases provided to Customer by Airbus DS Communications whether created by Airbus DS Communications or its third party licensors such as, without limitation, the mapping product databases) as well as information related to the business of Airbus DS Communications or Customer. Information will not include: (i) information publicly known prior to disclosure; (ii) information coming into the lawful possession of the recipient without any confidentiality obligation; and (iii) information required to be disclosed pursuant to regulatory action or court order, provided adequate prior written notice of any request to disclose is given to the Party whose information is to be disclosed. Each Party will exercise at least the same degree of care to safeguard the confidentiality of the other's Information as it does to safeguard its own proprietary confidential information, but not less than a reasonable degree of care.

10. **Infringement Indemnity.** With the exception of any third party software, hardware or equipment that may be provided under this Agreement, Airbus DS Communications agrees to hold Customer harmless from liability to third parties resulting from infringement of any United States patent or copyright or trade secret by the Airbus DS Communications software purchased hereunder and Airbus DS Communications further agrees to pay all damages and costs, including reasonable legal fees, which may be assessed against Customer under any such claim or action.

Service Agreement

Airbus DS Communications shall be released from the foregoing obligation unless Customer provides Airbus DS Communications with (i) written notice within fifteen (15) days of the date Customer first becomes aware of such a claim or action, or possibility thereof; (ii) sole control and authority over the defense or settlement thereof; and (iii) proper and full information and assistance to settle and/or defend any such claim or action. Without limiting the foregoing, if a final injunction is, or Airbus DS Communications believes, in its sole discretion, is likely to be, entered prohibiting the use of the software by Customer as contemplated herein, Airbus DS Communications will, at its sole option and expense, either (a) procure for Customer the right to use the infringing software as provided herein or (b) replace the infringing software with noninfringing, functionally equivalent products, or (c) suitably modify the infringing software so that it is not infringing; or (d) in the event (a), (b) and (c) are not commercially reasonable, terminate the license, accept return of the infringing software and refund to Customer an equitable portion of the license fee paid therefor. Except as specified above, Airbus DS Communications will not be liable for any costs or expenses incurred without its prior written authorization. Notwithstanding the foregoing, Airbus DS Communications assumes no liability for infringement claims with respect to software (i) not supplied by Airbus DS Communications, (ii) made in whole or in part in accordance to Customer's specifications, (iii) that is modified after delivery by Airbus DS Communications, (iv) combined with other products, processes or materials where the alleged infringement relates to such combination, (v) where Customer continues allegedly infringing activity after being notified thereof or after being informed of modifications that would have avoided the alleged infringement, or (vi) where Customer's use of the software is not strictly in accordance with this Agreement. THE FOREGOING PROVISIONS OF THIS SECTION STATE THE ENTIRE LIABILITY AND OBLIGATIONS OF AIRBUS DS COMMUNICATIONS AND THE EXCLUSIVE REMEDY OF CUSTOMER WITH RESPECT TO ANY ACTUAL OR ALLEGED INFRINGEMENT OF ANY PATENT, COPYRIGHT, TRADE SECRET, TRADEMARK OR OTHER INTELLECTUAL PROPERTY RIGHT BY THE SOFTWARE.

11. Injunctive Relief. Each Party acknowledges that a violation or threatened violation by it of Section 9 hereof would result in damage that is largely intangible but nonetheless real and that is incapable of complete remedy by award of damages. Thus, such violation or threatened violation will give the injured Party the right to a court-ordered injunction to specifically enforce such covenant or obligation. The Party in violation of any such section shall pay as damages reasonable expenses, including but not limited to attorney fees, incurred in obtaining specific enforcement.

12. Customer Indemnification. Customer shall indemnify, defend and hold Airbus DS Communications, its licensors and each such Party's parent organizations, subsidiaries, affiliates, officers, directors, employees, attorneys and agents harmless from and against any and all claims, costs, damages, losses, liabilities, and expenses (including attorneys' fees and costs) arising out of or in connection with: (i) A claim alleging that use of the Customer Data infringes the rights of, or has caused harm to a third party; (ii) a claim which if true, would constitute a violation by Customer of its representations and warranties contained herein; (iii) a claim arising from the breach by Customer of this Agreement, provided in any such case that Airbus DS Communications (a) gives Customer timely written notice of the claim; and (b) provides Customer all available information and assistance. Customer shall not settle or compromise any such claim without Airbus DS Communications' prior written consent.

13. Term. This Agreement will commence upon the Effective Date and shall continue until the end of the Initial Service Term as set forth in the Proposal. During the Initial Service Term, this Agreement shall not be terminable by Customer, except in instances of material breach (described below). Immediately following the Initial Service Term, this Agreement shall automatically renew for additional one (1) year terms ("Renewal Term") in accordance with Paragraph 2.2, above.

14. Termination.

14.1 Airbus DS Communications may terminate this Agreement without further obligation or liability to Customer if:

14.1.1 Customer fails to timely pay any amounts due under this Agreement and fails to make such payments within ten (10) days of written notice from Airbus DS Communications;

14.1.2 Customer commits any material breach of this Agreement and fails to remedy such breach within ten (10) days of written notice from Airbus DS Communications; or

AIRBUS DS COMMUNICATIONS

HOME OF VESTA™

Service Agreement

14.1.3 Customer becomes the subject of a petition in bankruptcy; is or becomes insolvent; or admits a general inability to pay its debts as they become due.

14.2 Customer may terminate this Agreement if Airbus DS Communications commits any material breach of this Agreement and fails to remedy such breach within thirty (30) days of written notice from Customer.

14.3 Upon termination or expiration of this Agreement, Customer shall be prohibited from further use of the Service and shall promptly return copies of any Documentation in its possession, if any, to Airbus DS Communications. All amounts owed to Airbus DS Communications, including but not limited to amounts due for setup services provided by Airbus DS Communications, shall be immediately due and payable, and Airbus DS Communications will cease performance of all obligations hereunder without liability to Customer. Sections 8, 9, 10, 11, 12, 14.3, 16 and 21 will survive termination or expiration. Upon termination, Customer shall have sixty (60) days to notify Airbus DS Communications if it opts to have Customer Data returned by Airbus DS Communications at the expense of Customer. In the event termination is due to Customer's failure to pay all fees due hereunder, Airbus DS Communications reserves the right to withhold return of Customer Data until paid in full. If Customer does not contact Airbus DS Communications during such 60 day timeframe and/or all fees are not paid current during that timeframe, Airbus DS Communications may destroy the Customer Data. Airbus DS Communications has no obligation to provide transition services in connection with Customer's election to utilize an alternative vendor.

15. Local Laws and Export Control. The Service utilizes Software and Technology that may be subject to United States export controls administered by the U.S. Department of Commerce, U.S. Department of State, U.S. Department of Treasury Office of Foreign Assets Control, and other U.S. agencies. The Customer acknowledges and agrees that the Service shall not be used, and none of the underlying information, Customer Data, Software, Documentation or Airbus DS Communications Technology may be transferred or otherwise exported or re-exported to countries as to which the United States maintains an embargo (collectively "Embargoed Countries"), or to or by a national or resident thereof, or any person or entity on the U.S. Department of Treasury's List of Specially Designated Nationals or the U.S. Department of Commerce's Table of Denial Orders (collectively, "Designated Nationals"). The lists of Embargoed Countries and Designated Nationals are subject to change without notice. By using the Service Customer represents and warrants that is not located in, under the control of, or a national or resident of an Embargoed Country or Designated National. Customer agrees to strictly comply with all U.S. export laws and assumes sole responsibility for obtaining licenses to export or re-export as may be required.

The Service may use encryption technology that is subject to licensing requirements under the U.S. Export Administration Regulations, 15. C.F.R. Parts 730-774 and Council Regulation (EC) No. 1334/2000. Airbus DS Communications and its licensors make no representation that the Service is appropriate or available for use in other locations. If Customer uses this Service from outside the United States, Customer is solely responsible for compliance with all applicable laws, including without limitation, export and import regulations of other countries. Any diversion of the Customer Data, Airbus DS Communications Technology and/or Content contrary to United States law is strictly prohibited.

16. Other Remedies. Airbus DS Communications' rights and remedies under this Agreement will be cumulative and in addition to all other rights and remedies available to Airbus DS Communications in law and in equity.

17. Assignment. Neither this Agreement nor any rights or duties hereunder may be transferred, assigned, sublicensed or otherwise disposed of by Customer to a third party, by operation of law or otherwise, without Airbus DS Communications' prior written consent. Notwithstanding the foregoing, Airbus DS Communications may assign its interests to a parent or affiliate company in the event of sale or merger of its assets so long as the acquiring entity agrees to assume all of Airbus DS Communications' duties and obligations hereunder.

18. Partial Invalidity. If any provision of this Agreement is ruled wholly or partly invalid or unenforceable by a court or other government body of competent jurisdiction, the validity and enforceability of all provisions of this Agreement not ruled to be invalid or unenforceable will be unaffected.

19. Modification; Waiver. Airbus DS Communications reserves the right to modify the terms and conditions of this Agreement or its policies relating to the Service at any time, effective upon posting of an updated version of this Agreement online. Customer is responsible for regularly reviewing this Agreement. Continued use of the Service after any such change shall constitute Customer's consent to such change. No term or condition of this Agreement

AIRBUS DS COMMUNICATIONS

brand of VESTA

Service Agreement

may be waived except in writing signed by the Party charged with waiver. A waiver will operate only as to the specific term or condition waived and will not constitute a waiver for the future.

20. Notice. All notices and other communications required or contemplated herein will be in writing and delivered either by (i) personal delivery; (ii) expedited messenger service; or (iii) postage prepaid return receipt requested certified mail; at the addresses first written above or such other address as the intended recipient previously has designated by written notice to the sender.

21. Governing Law. This Agreement will be governed exclusively by the laws of the State of California, without regard to its conflict of laws provisions. All parties agree that venue regarding any action arising hereunder will be exclusively in San Diego County, North County Judicial District, California.

22. Third Party Beneficiaries. None of the provisions of this Agreement is intended by the parties, nor shall they be deemed, to confer any benefit on any person not a Party to this Agreement.

23. Independent Contractors. The relationship of the parties hereunder will be one of independent contractors and not that of a franchise, joint venture or employer. Neither Party will have, and neither of them will represent to any other person that it has, any power, right or authority to bind the other, or to assume or create any obligation or responsibility, express or implied, on behalf of the other, except as expressly provided by this Agreement or as otherwise permitted in writing signed by both parties.

24. Entire Agreement. This Agreement and its schedules constitute the entire agreement of the parties with respect to the subject matter hereof, and supersede and cancel all prior agreements between the parties, written, oral or implied with respect to the subject matter hereof. The terms of any customer-provided purchase order or invoice concerning any product or service provided hereunder will not serve to replace, modify or supersede the terms of this Agreement. The terms of this Agreement shall prevail for any and all purposes.

25. Headings. Headings are included in this Agreement for convenience only and are not to be deemed to be part of this Agreement. The interpretation of this Agreement will not be affected by any heading herein.

26. Force Majeure. In the event an act of government, war, fire, flood, act of God, power shortages or blackouts, breakdown of telephone lines and services, failure of the Internet, or other causes beyond the reasonable control of Airbus DS Communications prevents Airbus DS Communications from performing in accordance with the terms of this Agreement, such nonperformance shall be excused and shall not be considered a breach or default for so long as such conditions prevail. AIRBUS DS COMMUNICATIONS' SERVICES MAY BE SUBJECT TO LIMITATIONS, DELAYS, AND OTHER PROBLEMS INHERENT IN THE USE OF THE INTERNET AND ELECTRONIC COMMUNICATIONS. AIRBUS DS COMMUNICATIONS IS NOT RESPONSIBLE FOR AND SHALL HAVE NO LIABILITY FOR SUCH DELAY, DELIVERY FAILURES OR OTHER DAMAGE RESULTING FROM SUCH PROBLEMS.

27. Marketing. Customer hereby provides its consent to be identified as a customer in sales announcements or other marketing material generated by Airbus DS Communications from time to time during the term of this Agreement.

28. Counterparts. This Agreement may be executed in one or more counterparts, all of which taken together shall constitute one instrument. Once fully executed, it will become effective as of the Effective Date stated above. Delivery of an executed signature page of this Agreement by facsimile transmission or electronic photocopy (i.e., "pdf") shall be equally effective as manual delivery of an original signed counterpart hereof.

AIRBUS DS COMMUNICATIONS

MODEL OF VESTA™

Service Agreement

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be signed by their authorized representatives as of the Effective Date.

Airbus DS Communications, Inc.

Customer

NH Department of Health & Human Services

By: _____
(Signature)

By: _____
(Signature)

Name: _____

Name: _____

Title: _____

Title: _____

REDACTED EXCERPT

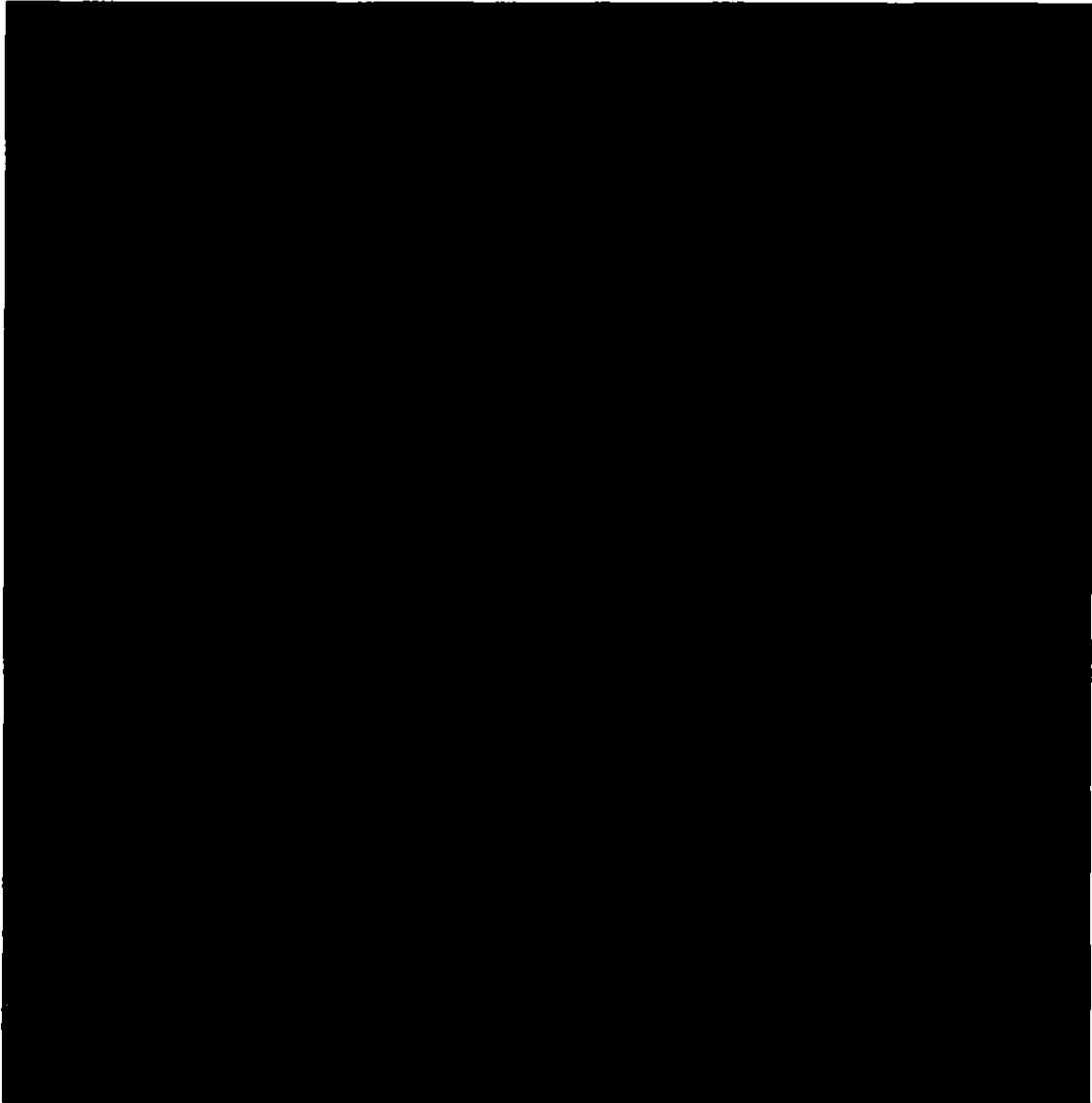
**AMENDED AND RESTATED BYLAWS
OF
AIRBUS DS COMMUNICATIONS, INC.**

TABLE OF CONTENTS

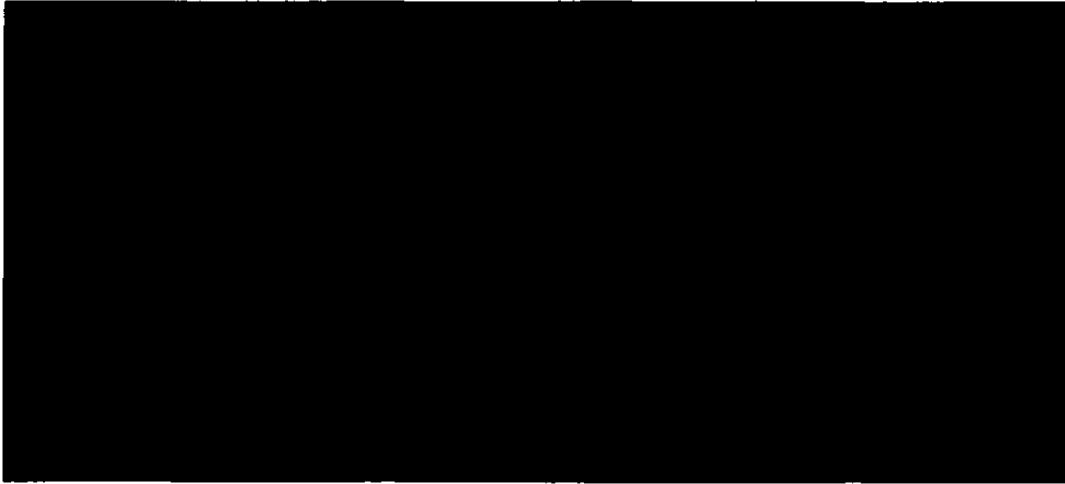
	Page
ARTICLE I. OFFICES	1
Section 1. PRINCIPAL OFFICES	1
Section 2. OTHER OFFICES	1
ARTICLE II. MEETINGS OF SHAREHOLDERS	1
Section 1. PLACE OF MEETINGS	1
Section 2. ANNUAL MEETINGS OF SHAREHOLDERS	1
Section 3. SPECIAL MEETINGS	1
Section 4. NOTICE OF SHAREHOLDERS' MEETINGS	2
Section 5. MANNER OF GIVING NOTICE; AFFIDAVIT OF NOTICE	2
Section 6. QUORUM	2
Section 7. ADJOURNED MEETING AND NOTICE THEREOF	2
Section 8. VOTING	3
Section 9. WAIVER OF NOTICE OR CONSENT BY ABSENT SHAREHOLDERS	3
Section 10. SHAREHOLDER ACTION BY WRITTEN CONSENT WITHOUT A MEETING	4
Section 11. RECORD DATE FOR SHAREHOLDER NOTICE, VOTING, AND GIVING CONSENTS	4
Section 12. PROXIES	5
Section 13. INSPECTORS OF ELECTION	5
ARTICLE III. DIRECTORS	6
Section 1. POWERS	6
Section 2. NUMBER AND QUALIFICATION OF DIRECTORS	6
Section 3. ELECTION AND TERM OF OFFICE OF DIRECTORS	6
Section 4. VACANCIES	6
Section 5. PLACE OF MEETINGS AND TELEPHONIC MEETINGS	7
Section 6. ANNUAL MEETINGS	7
Section 7. OTHER REGULAR MEETINGS	7
Section 8. SPECIAL MEETINGS	7
Section 9. DISPENSING WITH NOTICE	8
Section 10. QUORUM	8
Section 11. ADJOURNMENT	8
Section 12. NOTICE OF ADJOURNMENT	8
Section 13. ACTION WITHOUT MEETING	8
Section 14. FEES AND COMPENSATION OF DIRECTORS	8
ARTICLE IV. COMMITTEES	10
Section 1. COMMITTEES OF DIRECTORS	8
Section 2. MEETINGS AND ACTION OF COMMITTEES	9
ARTICLE V. OFFICERS	9
Section 1. OFFICERS	9
Section 2. ELECTION OF OFFICERS	9
Section 3. SUBORDINATE OFFICERS, ETC.	9
Section 4. REMOVAL AND RESIGNATION OF OFFICERS	10
Section 5. VACANCIES IN OFFICES	10
Section 6. CHAIRMAN OF THE BOARD	10

Section 7. PRESIDENT.....	10
Section 8. VICE PRESIDENTS.....	10
Section 9. SECRETARY.....	10
Section 10. TREASURER.....	11
ARTICLE VI. INDEMNIFICATION OF DIRECTORS, OFFICERS, EMPLOYEES AND OTHER AGENTS.....	11
ARTICLE VII. RECORDS AND REPORTS.....	12
Section 1. MAINTENANCE AND INSPECTION OF SHARE REGISTER.....	12
Section 2. MAINTENANCE AND INSPECTION OF BYLAWS.....	12
Section 3. MAINTENANCE AND INSPECTION OF OTHER CORPORATE RECORDS.....	12
Section 4. INSPECTION BY DIRECTORS.....	12
Section 5. ANNUAL REPORT TO SHAREHOLDERS.....	13
Section 6. FINANCIAL STATEMENTS.....	13
Section 7. ANNUAL STATEMENT OF GENERAL INFORMATION.....	13
ARTICLE VIII. GENERAL CORPORATE MATTERS.....	14
Section 1. RECORD DATE FOR PURPOSES OTHER THAN NOTICE AND VOTING.....	14
Section 2. CHECKS, DRAFTS, EVIDENCES OF INDEBTEDNESS.....	14
Section 3. CORPORATE CONTRACTS AND INSTRUMENTS; HOW EXECUTED.....	14
Section 4. CERTIFICATES FOR SHARES.....	14
Section 5. LOST CERTIFICATES.....	14
Section 6. REPRESENTATION OF SHARES OF OTHER CORPORATIONS.....	15
ARTICLE IX. AMENDMENTS.....	15
Section 1. AMENDMENT BY SHAREHOLDERS.....	15
Section 2. AMENDMENT BY DIRECTORS.....	15
ARTICLE X. GENERAL.....	15
Section 1. GOVERNING LAW.....	15
Section 2. CONSTRUCTION AND DEFINITIONS.....	15

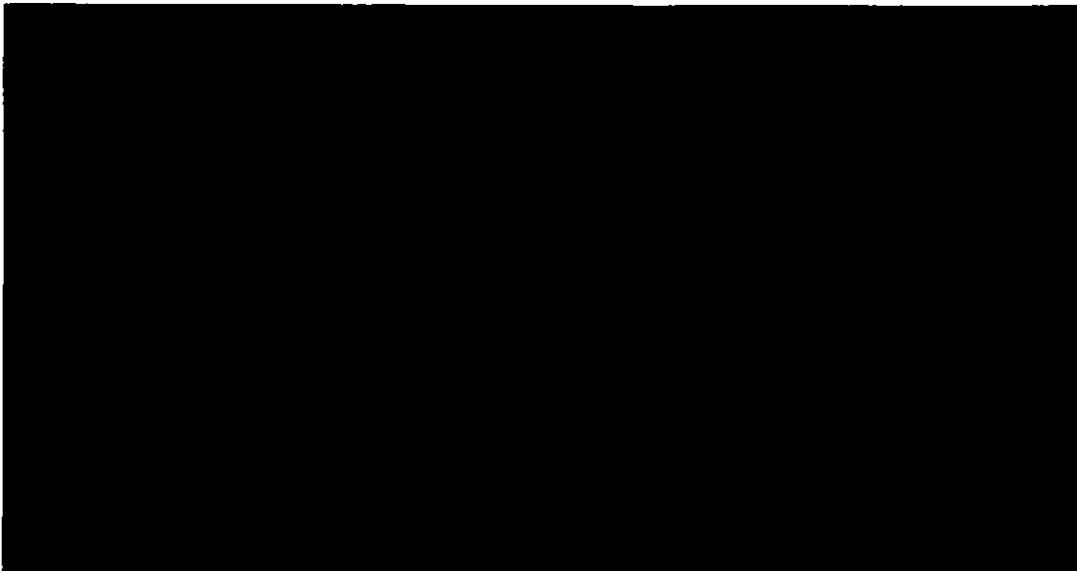
**AMENDED AND RESTATED BYLAWS
OF
AIRBUS DS COMMUNICATIONS, INC.
(Adopted as of August 1, 2014)**



**ARTICLE VIII.
GENERAL CORPORATE MATTERS**



3. **CORPORATE CONTRACTS AND INSTRUMENTS; HOW EXECUTED.** The Board of Directors, except as otherwise provided in these bylaws, may authorize any officer or officers, agent or agents, to enter into any contract or execute any instrument in the name of and on behalf of the corporation, and such authority may be general or confined to specific instances; and, unless so authorized or ratified by the Board of Directors or within the agency power of an officer, no officer, agent or employee shall have any power or authority to bind the corporation by any contract or engagement or to pledge its credit or to render it liable for any purpose or to any amount.



STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049

BUSINESS REQUIREMENTS					
State Requirements					
Req #	Requirement Description	Criticality			
SYSTEM FEATURES					
B1.1	Ability to manually add users.	M	Y	Standard	
B1.2	Ability to provide security levels for user roles: System Administrator, Creator, User, Roster User.	M	Y	Standard	
B1.3	Ability to import users from spreadsheets.	M	Y	Standard	
B1.4	Software accessible using a web browser.	M	Y	Standard	
B1.5	Access via desktop or remotely by phone for notifications.	M	Y	Standard	
B1.6	Ability to notify by contact groups.	M	Y	Standard	
B1.7	Ability to use mobile device, fax, telephone, email, pager for notifications.	M	Y	Standard	
B1.8	Up to 10 concurrent users on the system at the same time.	M	Y	Standard	
B1.9	Ability for security users to develop custom reports.	M	Y	Standard	
B1.10	Access to hosted backup: a secondary redundant system providing near real-time backup of the primary system.	M	Y	Standard	
B1.11	Ability to electronically fax users using the Efax solution.	M	Y	Standard	
USER REQUIREMENTS					
B2.1	Roster users have the ability to: view/edit personal contact information.	M	Y	Standard	
B2.2	Users have the ability to: view/edit personal contact information; view, modify and remove groups assigned to his/her department; view, modify, remove, activate and stop scenarios assigned to his/her department.	M	Y	Standard	

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049

APPLICATION REQUIREMENTS

State Requirements					
Req #	Requirement Description	Criticality			
APPLICATION SECURITY					
A1.1	Ability to access data using open standards access drivers (please specify supported versions in the comments field).	M	Y	Standard	
A1.2	Web-based compatible and in conformance with the following W3C standards:	M	N/A	N/A	
A1.3	XHTML 1.0	M	Y	Standard	
A1.4	CSS 2.1	M	Y	Standard	
A1.5	Verify the identity and authorize all of the system users before allowing use of the system to prevent access to inappropriate or confidential data or services.	M	Y	Standard	
A1.6	Verify the identity and authenticate all of the system's users before allowing them to use its capabilities to prevent access to inappropriate or confidential data or services.	M	Y	Standard	
A1.7	Enforce unique user names.	M	Y	Standard	
A1.8	Enforce complex passwords for Administrator Accounts of ten characters or more in accordance with DoIT's statewide <i>User Account and Password Policy</i> .	M	Y	Standard	
A1.9	Enforce the use of complex passwords for general users using capital letters, numbers and special characters.	M	Y	Standard	
A1.10	Encrypt passwords in transmission and at rest within the database.	M		Standard	
A1.11	Expire passwords after a definite period of time.	M	Y	Standard	
A1.12	Authorize users and client applications to prevent access to inappropriate or confidential data or services.	M	Y	Standard	
A1.13	Provide ability to limit the number of people that can grant or change authorizations.	M	Y	Standard	
A1.14	Establish ability to enforce session timeouts during periods of inactivity.	M	Y	Standard	

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049

A1.15	Ensure application has been tested and hardened to prevent critical application security flaws. (At a minimum, the application shall be tested against all flaws outlined in the Open Web Application Security Project (OWASP) Top Ten (http://www.owasp.org/index.php/OWASP_Top_Ten_Project))	M	Y	Standard	
A1.16	The application shall not store authentication credentials or sensitive Data in its code.	M	Y	Standard	
A1.17	Audit all attempted accesses that fail identification, authentication and authorization requirements.	M	N	Not Available	
A1.18	The application shall log all activities to a central server to prevent parties to application transactions from denying that they have taken place. The logs must be kept for 30 days.	M	Y	Standard	
A1.19	The application must allow a user to explicitly terminate a session. No remnants of the prior session should then remain.	M		Standard	
A1.20	Use only the Software and System Services designed for use.	M	Y	Standard	
A1.21	The application Data shall be protected from unauthorized use when at rest.	M	Y	Standard	
A1.22	Keep any sensitive Data or communications private from unauthorized individuals and programs.	M	Y	Standard	
A1.23	Subsequent application enhancements or upgrades shall not remove or degrade security requirements.	M	Y	Standard	
A1.24	Create change management documentation and procedures.	M	Y	Standard	

TESTING					
State Requirements					
Req #	Requirement Description	Criticality			
APPLICATION SECURITY TESTING					
T1.1	All components of the Software shall be reviewed and tested to ensure they protect the State's web site and its related Data assets.	M	Y	Standard	
T1.2	The Vendor shall be responsible for security testing, as appropriate. Tests shall focus on the technical, administrative and physical security controls that have been designed into the System architecture in order to provide the necessary confidentiality, integrity and availability.	M	Y	Standard	
T1.3	Test for Identification and Authentication; supports obtaining information about those parties attempting to log onto a system or application for security purposes and the validation of users.	M	Y	Standard	Multiple security tests shall be performed on a periodic basis and include, Basic Network, Host Discovery, Heartbleed, PatchAudit, PCI, Windows Malware, and Database Security
T1.4	Test for Access Control; supports the management of permissions for logging onto a computer or network.	M	Y	Standard	
T1.5	Test for encryption; supports the encoding of data for security purposes.	M	Y	Standard	

TESTING					
State Requirements					
Req #	Requirement Description	Criticality			
APPLICATION SECURITY TESTING					
T1.6	Test the Intrusion Detection; supports the detection of illegal entrance into a computer system.	M	Y	Standard	Airbus shall use a third party IDS appliance and service (BAE Systems, formally SilverSky) to monitor network traffic
T1.7	Test the Verification feature; supports the confirmation of authority to enter a computer system, application or network.	M	Y	Standard	
T1.8	Test the Digital Signature; guarantees the unaltered state of a file.	M	Y	Standard	Production systems shall be built against a standard release base line and are monitored for changes using several criteria which include Core Attributes, Size, as well as Checksums in addition to our ongoing system access monitoring.
T1.9	Test the User Management feature; supports the administration of computer, application and network accounts within an organization.	M	Y	Standard	
T1.10	Test Role/Privilege Management; supports the granting of abilities to users or groups of users of a computer, application or network.	M	Y	Standard	
T1.11	Test Audit Trail Capture and Analysis; supports the identification and monitoring of activities within an application or system.	M	Y	Standard	
T1.12	Test Input Validation; ensures the application is protected from buffer overflow, cross-site scripting, SQL injection, and unauthorized access of files and/or directories on the server.	M	Y	Standard	

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049

TESTING					
State Requirements					
Req #	Requirement Description	Criticality			
APPLICATION SECURITY TESTING					
T1.13	Provide the State with validation of 3rd party penetration testing performed on the application and system environment.	M	Y	Standard	
T1.14	Prior to the System being moved into production, the Vendor shall provide results of all security testing to the Department of Information Technology for review and acceptance.	M	Y	Standard	
T1.15	The Vendor must provide validation that 3rd party penetration testing has been performed on the current software version and hardware configuration.	M	Y	Standard	
T1.16	The Vendor must perform application testing using an industry standard and State approved testing methodology.	M	Y	Standard	Airbus shall use a number of industry standard applications such as AppDetective, Nessus, and Qualys. State recommendations for additional applications that are not included in the standard service shall be considered.
T1.17	All testing results must be shared with the State.	M	Y	Standard	Test results specific to the State's production environment and applications shall be provided on Go Live and upon any significant application modifications.
T1.18	The Vendor must perform application stress testing and tuning.	M	Y	Standard	
STANDARD TESTING					
T2.1	Installation Testing.	M	Y	Standard	
T2.2	User Acceptance Testing (UAT).	M	Y	Standard	

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049

TESTING				
State Requirements				
Req #	Requirement Description	Criticality		
APPLICATION SECURITY TESTING				
T2.3	Performance Tuning and Stress Testing.	M	Y	Standard

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049

HOSTING-CLOUD REQUIREMENTS					
State Requirements					
Req #	Requirement Description	Criticality			
OPERATIONS					
H1.1	Vendor shall maintain a secure hosting environment providing all necessary hardware, software, and Internet bandwidth to manage the application and support users with permission based logins.	M	Y	Standard	
H1.2	State access will be via Internet Browser.	M	Y	Standard	
H1.3	At a minimum, the System should support Microsoft IE Version 9 and above.	M	Y	Standard	
H1.4	The State will be responsible for equipment, labor, and /or services necessary to set-up and maintain the internet connectivity at the State and/or other third party sites.	M	Y	Standard	
H1.5	Vendor will not be responsible for network connection issues, problems or conditions arising from or related to circumstances outside the control of the Vendor, ex: bandwidth, network outages and /or any other conditions arising on the State's internal network or, more generally, outside the Vendor's firewall or any issues that are the responsibility of the State Internet Service Provider.	M	Y	Standard	
H1.6	Vendor shall provide a secure Class A Data Center providing equipment (including dedicated servers), an on-site 24/7 system operator, managed firewall services, and managed backup Services.	M	Y	Standard	
H1.7	Data Center Air Conditioning – used to control temperature and humidity in the Data Center. Temperature ranges shall be between 68 and 75 °F.	M	Y	Standard	
H1.8	Data Center Humidity shall be non-condensing and be maintained between 40-55% with a maximum dew point of 62 °F.	M	Y	Standard	
H1.9	Data Center Backup Power – uninterruptible power supplies shall be sized to sustain computer systems and associated components for, at a minimum, the amount of time it takes for a backup generator to take over providing power. Where possible, servers shall contain redundant power supplies connected to commercial power via separate feeds.	M	Y	Standard	

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049

HOSTING-CLOUD REQUIREMENTS					
State Requirements					
Req #	Requirement Description	Criticality			
H1.10	Data Center Generator – shall be sufficient to sustain computer systems and associated components for, at a minimum, the amount of time it takes for commercial power to return. Fuel tanks shall be large enough to support the generator at full load for a period not less than 1 % days of operation.	M	Y	Standard	
H1.11	Data Center Floor – A raised floor is required for more uniform air circulation in the form of a plenum for cold air as well as to provide space for power cabling and wetness monitoring.	M	Y	Standard	
H1.12	Data Center Fire Protection System – fire detectors in conjunction with suppression gaseous systems must be installed to reduce the risk of loss due to fire.	M	Y	Standard	
H1.13	The Data Center must be physically secured – restricted access to the site to personnel with controls such as biometric, badge, and others security solutions. Policies for granting access must be in place and followed. Access shall only be granted to those with a need to perform tasks in the Data Center.	M	Y	Standard	
H1.14	Vendor must monitor the application and all servers.	M	Y	Standard	
H1.15	Vendor shall manage the databases and services on all servers located at the Vendor's facility.	M	Y	Standard	
H1.16	Vendor shall install and update all server patches, updates, and other utilities within 60 days of release from the manufacturer.	M	Y	Standard	
H1.17	Vendor shall monitor System, security, and application logs.	M	Y	Standard	
H1.18	Vendor shall manage the sharing of data resources.	M	Y	Standard	
H1.19	Vendor shall manage daily backups, off-site data storage, and restore operations.	M	Y	Standard	

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049

HOSTING-CLOUD REQUIREMENTS					
State Requirements			Vendor		
Req #	Requirement Description	Criticality	Vendor Response	Delivery Method	Comments
H1.20	The Vendor shall monitor physical hardware.	M	Y	Standard	
H1.21	The Vendor shall immediately report any breach in security to the State of New Hampshire.	M	Y	Standard	
DISASTER RECOVERY					
H2.1	Vendor shall conform to adequate disaster recovery procedures as defined by the State of New Hampshire.	M	Y	Standard	For resiliency of the production environment Airbus shall use two geographically separate third party data centers to provide physical and environmental security for two totally independent purpose built networks and server infrastructure. Both environments shall be maintained active and receive encrypted database update on a periodic bases, typically every four hours.
H2.2	Vendor shall have documented disaster recovery plans that address the recovery of lost State data as well as their own. Systems shall be architected to meet the defined recovery needs.	M	Y	Standard	
H2.3	The disaster recovery plan shall identify appropriate methods for procuring additional hardware in the event of a component failure. In most instances, systems shall offer a level of redundancy so the loss of a drive or power supply will not be sufficient to terminate services however, these failed components will have to be replaced.	M	Y	Standard	
H2.4	Vendor shall adhere to a defined and documented back-up schedule and procedure.	M	Y	Standard	
H2.5	Back-up copies of data are made for the purpose of facilitating a restore of the data in the event of data loss or System failure.	M	Y	Standard	
H2.6	Scheduled backups of all servers must be completed regularly. At a minimum, Bluehost servers shall be backed up nightly, with one daily, one weekly, and one monthly backup stored in a secure location to assure data recovery in the event of disaster.	M	Y	Standard	

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049

HOSTING-CLOUD REQUIREMENTS					
State Requirements			Vendor		
Req #	Requirement Description	Criticality	Vendor Response	Delivery Method	Comments
H2.7	The minimum acceptable frequency is differential backup daily, and complete backup weekly.	M	Y	Standard	
H2.8	Tapes or other back-up media tapes must be securely transferred from the site to another secure location to avoid complete data loss with the loss of a facility.	M	Y	Standard	
H2.9	If State data is personally identifiable, data must be encrypted in the operation environment and on back up tapes.	M	Y	Standard	Database servers shall be maintained separately from the externally facing web application servers and shall not have external IP addresses. All data shall be encrypted during transport or at rest with the exception of realtime data needed for use within the active notification application where only password data is encrypted. Data transfer between data centers shall be encrypted/decrypted prior to VPN transport and Disaster Recovery tape backups shall be encrypted during the tape backup process.
H2.10	Data recovery - In the event that recovery back to the last backup is not sufficient to recover State Data, the Vendor shall employ the use of database logs in addition to backup media in the restoration of the database(s) to afford a much closer to real-time recovery. To do this, logs must be moved off the volume containing the database with a frequency to match the business needs.	M	Y	Standard	Every 4 hours
NETWORK ARCHITECTURE					
H3.1	The Vendor must operate hosting Services on a network offering adequate performance to meet the business requirements for the State application. For the purpose of this RFP, adequate performance is defined as 99.9% uptime, exclusive of the regularly scheduled maintenance window.	M	Y	Standard	
H3.2	The Vendor shall provide network redundancy deemed adequate by the State by assuring redundant connections provided by multiple Internet Vendors, so that a failure of one Internet connection will not interrupt access to the State application.	M	Y	Standard	

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049

HOSTING-CLOUD REQUIREMENTS					
State Requirements					
Req #	Requirement Description	Criticality	Vendor Response	Industry Standard	Comments
H3.3	The Vendor' network architecture must include redundancy of routers and switches in the Data Center.	M	Y	Standard	
SECURITY					
H4.1	The Vendor shall employ security measures ensure that the State's application and data is protected.	M	Y	Standard	
H4.2	If State data is hosted on multiple servers, data exchanges between and among servers must be encrypted.	M	Y	Standard	
H4.3	All servers and devices must have currently-supported and hardened operating systems, the latest anti-viral, anti-hacker, anti-spam, anti-spyware, and anti-malware utilities. The environment, as a whole, shall have aggressive intrusion-detection and firewall protection.	M	Y	Standard	
H4.4	All components of the Infrastructure shall be reviewed and tested to ensure they protect the State's hardware, software, and its related data assets. Tests shall focus on the technical, administrative and physical security controls that have been designed into the System architecture in order to provide confidentiality, integrity and availability.	M	Y	Standard	
H4.5	In the development or maintenance of any code, the Vendor shall ensure that the Software is independently verified and validated using a methodology determined appropriate by the State. All software and hardware shall be free of malicious code.	M	Y	Standard	
H4.6	The Vendor shall notify the State's Project Manager of any security breaches within two (2) hours of the time that the Vendor learns of their occurrence.	M	Y	Standard	
H4.7	The Vendor shall ensure its complete cooperation with the State's Chief Information Officer in the detection of any security vulnerability of the Vendor' hosting Infrastructure and/or the application.	M	Y	Standard	
H4.8	The Vendor shall be solely liable for costs associated with any breach of State data housed at their location(s) including but not limited to notification and any damages assessed by the courts.	M	Y	Standard	
H4.9	The Vendor shall authorize the State to perform scheduled and random security audits, including vulnerability assessments, of the Vendor' hosting Infrastructure and/or the application upon request.	M	Y	Standard	

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049

HOSTING-CLOUD REQUIREMENTS					
State Requirements			Vendor		
Req #	Requirement Description	Criticality	Vendor Response	Delivery Standard	Comments
H4.10	Logging should go to centralized logs server for security reasons. Logs should include System, Application, Web and Database logs.	M	Y	Standard	
H4.11	The operating system and the data base should be built and hardened wherever possible to guidelines set forth by: CIS (Center Internet Security), NIST, and NSA.	M	Y	Standard	
H4.12	The Vendor must provide reports to validate that redundancy is in fact in place and backup/restores are functioning.	M	Y	Standard	
H4.13	The Vendor shall provide fire detection and suppression system, physical security of and infrastructure security of the proposed hosting facility. The environmental support equipment of the Vendor website hosting facility: power conditioning; HVAC; UPS; generator must be acceptable to the State.	M	Y	Standard	
SERVICE LEVEL AGREEMENT					
H5.1	The Vendor's System support and maintenance shall commence upon the Effective Date and extend through the end of the Contract term, and any extensions thereof.	M	Y	Standard	
H5.2	Maintain the hardware and Software in accordance with the Specifications, terms, and requirements of the Contract, including providing, upgrades and fixes as required.	M	Y	Standard	
H5.3	Repair or replace the hardware or Software, or any portion thereof, so that the System operates in accordance with the Specifications, terms, and requirements of the Contract.	M	Y	Standard	
H5.4	The State shall have unlimited access, via phone or Email, to the Vendor technical support staff between the hours of 8:30am to 5:00pm- Monday thru Friday EST;	M	Y	Standard	

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049

HOSTING-CLOUD REQUIREMENTS					
State Requirements			Vendor		
Req #	Requirement Description	Criticality	Vendor Response	Delivery Method	Comments
HS.5	The Vendor response time for support shall conform to the specific deficiency class as described below: <ul style="list-style-type: none"> Class A Deficiency - Software - Critical, does not allow System to operate, no work around, demands immediate action; Written Documentation - missing significant portions of information or unintelligible to State; Non Software - Services were inadequate and require re-performance of the Service. Class B Deficiency - Software - important, does not stop operation and/or there is a work around and user can perform tasks; Written Documentation - portions of information are missing but not enough to make the document unintelligible; Non Software - Services were deficient, require reworking, but do not require re-performance of the Service. Class C Deficiency - Software - minimal, cosmetic in nature, minimal effect on System, low priority and/or user can use System; Written Documentation - minimal changes required and of minor editing nature; Non Software - Services require only minor reworking and do not require re-performance of the Service. 	M	Y	Standard	
HS.6	As part of the Software maintenance agreement, ongoing software maintenance and support issues, shall be responded to according to the following: <ul style="list-style-type: none"> a. Class A Deficiencies - The Vendor shall have available to the State on-call telephone assistance, with issue tracking available to the State, eight (8) hours per day and five (5) days a week with an email / telephone response within two (2) hours of request; or the Vendor shall provide support on-site or with remote diagnostic Services, within four (4) business hours of a request; b. Class B & C Deficiencies - The State shall notify the Vendor of such Deficiencies during regular business hours and the Vendor shall respond back within four (4) hours of notification of planned corrective action; The Vendor shall repair or replace Software, and provide maintenance of the Software in accordance with the Specifications, Terms and Requirements of the Contract; 	M	Y	Standard	
HS.7	The hosting server for the State shall be available twenty-four (24) hours a day, 7 days a week except for during scheduled maintenance.	M	Y	Standard	
HS.8	The Vendor will guide the State with possible solutions to resolve issues to maintain a fully functioning, hosted System.	M	Y	Standard	

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049

HOSTING-CLOUD REQUIREMENTS					
State Requirements			Vendor		
Req #	Requirement Description	Criticality	Vendor Response	Delivery Method	Comments
HS.9	A regularly scheduled maintenance window shall be identified (such as weekly, monthly, or quarterly) at which time all relevant server patches and application upgrades shall be applied.	M	Y	Standard	
HS.10	The Vendor response time for support shall conform to the specific deficiency class as described in HS.6.	M	Y	Standard	Regular and Emergency Telephone Support 8AM – 5PM Monday - Friday
HS.11	DEFICIENCIES ARE STATED in HS.5.	M	Y	Standard	After Hours On-Call Telephone Support is available for Emergencies Only from 5PM – 8AM Monday - Friday, Holidays, and Weekends.
HS.12	The Vendor will give two-business days prior notification to the State Project Manager of all changes/updates and provide the State with training due to the upgrades and changes.	M	Y	Standard	
HS.13	The Vendor shall guarantee 99.9% uptime, exclusive of the regularly scheduled maintenance window.	M	Y	Standard	

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049

HOSTING-CLOUD REQUIREMENTS					
State Requirements			Vendor		
Req #	Requirement Description	Criticality	Vendor Response	Delivery Method	Comments
HS.14	If The Vendor is unable to meet the 99.9% uptime requirement, The Vendor shall credit State's account in an amount based upon the following formula: $(\text{Total Contract Item Price}/365) \times \text{Number of Days Contract Item Not Provided}$. The State must request this credit in writing.	M	Y	Standard	
HS.15	The Vendor shall use a change management policy for notification and tracking of change requests as well as critical outages.	M	Y	Standard	
HS.16	A critical outage will be designated when a business function cannot be met by a nonperforming application and there is no work around to the problem.	M	Y	Standard	

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049

HOSTING-CLOUD REQUIREMENTS					
State Requirements			Vendor		
Req #	Requirement Description	Criticality	Vendor Response	Delivery Method	Comments
H5.17	All hardware and software components of the Vendor hosting infrastructure shall be fully supported by their respective manufacturers at all times. All critical patches for operating systems, databases, web services, etc, shall be applied within sixty (60) days of release by their respective manufacturers.	M	Y	Standard	
H5.18	The Vendor shall maintain a record of the activities related to repair or maintenance activities performed for the State and shall report quarterly on the following: Server up-time; All change requests implemented, including operating system patches; All critical outages reported including actual issue and resolution; Number of deficiencies reported by class with initial response time as well as time to close.	M	Y	Standard	
H5.19	The Vendor shall provide the State with a personal secure FTP site to be used the State for uploading and downloading files.	M	Y	Standard	

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049

SUPPORT & MAINTENANCE REQUIREMENTS					
State Requirements			Vendor		
Req #	Requirement Description	Criticality	Vendor Response	Delivery Method	Comments
SUPPORT & MAINTENANCE REQUIREMENTS					
S1.1	The Vendor's System support and maintenance shall commence upon the Effective Date and extend through the end of the Contract term, and any extensions thereof.	M	Y	Standard	
S1.2	Maintain the hardware and Software in accordance with the Specifications, terms, and requirements of the Contract, including providing, upgrades and fixes as required.	M	Y	Standard	
S1.3	Repair or replace the hardware or Software, or any portion thereof, so that the System operates in accordance with the Specifications, terms, and requirements of the Contract.	M	Y	Standard	
S1.4	The State shall have unlimited access, via phone or Email, to the Vendor technical support staff between the hours of 9:00 am to 6:00 pm- Monday thru Friday EST;	M	Y	Standard	
S1.5	The Vendor response time for support shall be 8 business hours for email response with a 15 minute call back targeted; 4 hour response to telephone inquiries as described in H5.6.	M	Y	Standard	
S1.6	The Vendor will guide the State with possible solutions to resolve issues to maintain a fully functioning, hosted System.	M	Y	Standard	
S1.7	The Vendor shall update the State's Hosted environment with the latest program updates, general maintenance releases, selected functionality releases, patches, and Documentation that are generally offered to its customers, at no additional cost.	M	Y	Standard	
S1.8	The Vendor shall maintain a record of the activities related to warranty repair or maintenance activities performed for the State;	M	Y	Standard	

Contract 2015-049 Attachment 2 - Contract Requirements

Initial and Date All Pages

Airbus Initials: RCDate: 7-21-2015

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049

SUPPORT & MAINTENANCE REQUIREMENTS					
State Requirements			Vendor		
Req #	Requirement Description	Criticality	Vendor Response	Delivery Method	Comments
S1.9	For all maintenance service calls, The Vendor shall ensure the following information will be collected and maintained: 1) nature of the Deficiency; 2) current status of the Deficiency; 3) Deficiency resolution information; 4) Resolved by; 5) Identifying number i.e., work order number; and, 6) Issue identified by. The following are collected only with Support Escalations: 7) action plans, dates and times; and, 8) expected and actual completion time.	M	Y	Standard	
S1.10	The Vendor must work with the State to identify and troubleshoot potentially large-scale System failures or Deficiencies by collecting the following information: 1) mean time between reported Deficiencies with the Software; 2) diagnosis of the root cause of the problem; and 3) identification of repeat calls or repeat Software problems.	M	Y	Standard	
WARRANTY SERVICES					
S2.1	Maintain the System Software in accordance with the Specifications and Terms of the Contract;	M	Y	Standard	
S2.2	Repair or replace the System Software or any portion thereof so that the System operates in accordance with the Specifications, terms and requirements of the Contract;	M	Y	Standard	
S2.3	Support On-Call is available 24/7 for Emergency Only with a 15 minute telephone response after receipt of message from the answering service. Email is not checked outside of business hours and is not recommended for emergencies. All other inquiries are handled during business hours.	M	Y	Standard	

Contract 2015-049 Attachment 2 - Contract Requirements

Initial and Date All Pages

Airbus Initials: RLDate: 7-24-2015

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049

SUPPORT & MAINTENANCE REQUIREMENTS					
State Requirements			Vendor		
Req #	Requirement Description	Criticality	Vendor Response	Delivery Method	Comments
S2.4	Maintain a record of the activities related to warranty repair or maintenance activities performed for the State;	M	Y	Standard	
S2.5	The Vendor must work with the State to identify and troubleshoot potentially large-scale Software failures or Deficiencies by collecting the following information: 1) mean time between reported Deficiencies with the Software; 2) diagnosis of the root cause of the problem; and 3) identification of repeat calls or repeat Software problems.	M	Y	Standard	

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
COMMUNICATOR HOSTING MAINTENANCE AND SUPPORT SERVICES
CONTRACT 2015-049

PROJECT MANAGEMENT					
State Requirements			Vendor		
Req #	Requirement Description	Criticality	Vendor	Delivery Method	Comments
PROJECT MANAGEMENT					
P1.1	Vendor shall participate in an initial kick-off meeting to initiate the Project.	M	Y	Standard	
P1.2	Vendor shall provide Project Staff as specified in the contract.	M	Y	Standard	
P1.3	Vendor shall submit a finalized Work Plan within ten (10) days after Contract award and approval by Governor and Council. The Work Plan shall include, without limitation, a detailed description of the Schedule, tasks, Deliverables, critical events, task dependencies, and payment Schedule. The plan shall be updated no less than weekly or as specified in the Work Plan.	M	Y	Standard	
P1.4	Vendor shall provide detailed weekly or as specified in the Work Plan status reports on the progress of the Project, which will include expenses incurred year to date.	M	Y	Standard	
P1.5	All user, technical, and System Documentation as well as Project Schedules, plans, status reports, and correspondence must be maintained as project documentation.	M	Y	Standard	

Airbus DS Communications Hosting Center Policies

Prepared By

Document Owner(s)	Project/Organization Role
Allen Van Meter	Director Hosted Services

Manual Version Control

Version	Date	Author	Change Description
1	3/31/2006	Allen Van Meter	Post review compilation of existing policies and updates based on the relocation of the hosting facility to Inflow's (now Sungard's) Nashville Internet Data Center, formal definition of a number of previously informal activities, and a more active role for Customer Support in the Hosting Center Operations decision process.
1.1	5/2/2006	Allen Van Meter	Update Customer Support Procedures and minor text edits.
1.2	11/21/06	Allen Van Meter	Minor text and format edits.
1.3	1/04/07	Allen Van Meter	Minor text and format edits.
1.4	09/26/07	Allen Van Meter	Minor text and format edits.
1.5	06/30/08	Allen Van Meter	Minor text and format edits.
1.6	7/15/10	Allen Van Meter	Minor text and format edits.
1.7	3/1/11	Allen Van Meter	Minor text and format edits. Include new dba designation of Airbus DS Communications.
1.8	2/7/12	Allen Van Meter	Minor text and format edits.
1.9	1/16/13	Allen Van Meter	Minor text and format edits.
2.0	10/17/14	Allen Van Meter	Company Name Change

Note The content of a manual does not constitute nor should it be construed as a contract between Airbus DS Communications and any of its clients.

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

RC
7-21-2006

Airbus DS Communications Hosting Center

Airbus DS Communications at its option, may change, delete, suspend, or discontinue parts of the policy in its entirety, at any time without prior notice. Any modifications will be conveyed to our clients after each review period.

Table of Contents

Table of Contents.....	2
Introduction.....	4
Airbus DS Communications' Hosting Business Resiliency Overview.....	5
Security Policy Summary.....	6
Security Procedures Summary.....	13
Anti-Virus Policy.....	20
Guidelines on Anti-Virus Process.....	21
Backup Policy.....	22
Business Continuity Policy.....	23
Change Management Policy.....	28
Change Management Procedure.....	30
Customer Support Procedures.....	39
Data Privacy Policy.....	44
Data Security Policy.....	45
Email Security Policy.....	47
Employee/Contractor Termination Procedure.....	48
Encryption Policy.....	49
Facility Access Control Policy.....	51
Information Classification & Distribution Policy.....	52
Network Security Policy.....	56
Password Policy.....	57
Personnel Screening Policy.....	60
Remote Access Policy.....	62
Security Awareness and Training Policy.....	65
Security Review and Audit Policy.....	67
Security Testing Policy.....	70
Security Violation Policy.....	72
Server Security Policy.....	73
Service Problem & Critical Incident Management Policy.....	76
Prioritizing Service Problems Procedure.....	78
Critical Incident Management Procedure.....	81
Software Maintenance Policy.....	84
System Monitoring Policy.....	86
Virtual Private Network (VPN) Policy.....	89

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

AC
7-11-10K

Airbus DS Communications Hosting Center

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

hc
2-21-2015

Airbus DS Communications Hosting Center

Introduction

This document has been developed by the Hosting Center Department in order to familiarize employees, clients, and vendors with the Airbus DS Communications Hosting Center and provide information about key policies and procedures affecting services provided.

1.0 History

Airbus DS Communications has provided hosted services to its clients for a number of years. Initially the hardware used to provide these services were located in a dedicated secure facility located within our corporate offices. We have since relocated all of our production servers to one of two managed data center facilities. The primary facility is located in Brentwood, TN and is operated by Peak10. The second facility is located in Mesa, AZ and is operated by AT&T. Each of these facilities provides a high level of physical security and environmental controls. Because each location is unique and maintains their own sets of policies and procedures, we have not attempted to capture the specifics within this document but details are available upon request. Site visits to each of the facilities can also be scheduled upon request.

2.0 Changes in Policy

This manual supersedes all previous Airbus DS Communications Hosting Center policy documents.

While every effort is made to keep the contents of this document current and clients informed of any changes that might impact services, Airbus DS Communications reserves the right to modify, suspend, or terminate any of the policies, and/or procedures, and/or benefits described in the manual with or without prior notice to clients.

3.0 Policy Reviews

Airbus DS Communications Hosting Center plans to review and update these policies on a quarterly basis. Meetings will also be held with all Airbus DS Communications Hosting Center Infrastructure and Support staff to discuss all policies as a whole, any modifications, and in preparation for the next quarterly review.

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

Mc
7-26-14

Airbus DS Communications' Hosting Business Resiliency Overview

Airbus DS Communications' hosting operations are deployed in data center facilities in Brentwood, TN and Mesa, AZ. These hosting operations employ co-production architecture, with both live customers and back-up systems housed in each facility. No facility is "all-backup" or "all-active". This ensures that infrastructure is continuously exercised to confirm "real-life" operational status versus a hypothetical automated test confirmation that might miss key system aspects.

In addition to normal traffic, automated tests run at least four times daily for Communicator! (CFW) systems and work is in progress to provide the same tests for the Communicator!@ NXT™ systems.

These tests exercise:

- Inbound activation lines
- Call-out capability
- Inbound callback lines
- The Communicator! Software (engine, database, etc.)

Any abnormal result, during automated testing, triggers an immediate alert to the Hosting Infrastructure team.

Airbus DS Communications' facilities share no common infrastructure (including local networks, phone service, switches, servers, databases, etc.) in order to insure that no single failure can render both a primary and a back-up server unavailable.

The company's hosted Communicator! NXT service includes web and phone access to a complete shared back-up system with calling capability and updates via Airbus DS Communications' DataSync service. DataSync automatically updates each customer's hosted back-up solution with data from the primary system every four hours. Also, because DataSync back-ups are stored at the off-site system, they are immediately available for emergency data recovery of the primary system – usually long before normal back-up media can be brought online.

All Hosted customer data is backed up daily, and media is rotated off-site weekly to ensure "worst case" recoverability.

All Airbus DS Communications servers are monitored by Mercury™ Sitescope to verify web accessibility and to ensure that the operating system is performing within normal parameters (e.g., disk space, processor utilization, etc.).

Hosted servers are monitored using HP's Insight Manager, which provides early notification of potential component failure. This ensures that Airbus DS Communications' Hosting Infrastructure team can take proactive measures to advert downtime due to hardware failure *before* it happens.

Security Policy Summary

1.0 Purpose

This document is intended as a comprehensive policy summary for securing Airbus DS Communications hosted customer systems, data, and communications (voice and data). This policy should guide the development of detailed security subject-area policy statements, as well as installation, configuration, and administrative procedures intended to secure these customer's systems and data.

2.0 Scope

These policies apply to all Airbus DS Communications employees, contractors, and third-party entities responsible for the installation, configuration, administration, and transportation of hosted customer systems and data. No individual who supports these entities or processes shall be exempt from these policies.

3.0 Policy

The following are security related subjects that must be addressed to provide a comprehensive security strategy for customer-hosted systems, data, and communications. These policies shall guide the development of detailed policy statements and their subsequent procedure documents. The following policies are only intended to summarize each security subject area. For an in-depth review of each of these policies, see the associated section by the same name within this document.

Anti-Virus Protection Policy

This policy establishes requirements that must be met by all computers connected to Airbus DS Communications hosting center networks to ensure effective virus detection and prevention.

All Airbus DS Communications PC-based Hosting Center servers, and connected workstations, must have Airbus DS Communications standard, supported anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus pattern files must apply critical updates within two weeks of their release. Virus-infected computers will be removed from the network until they are verified virus-free. Airbus DS Communications reserves the right to prosecute anyone who intentionally attempts to introduce malicious programs into Airbus DS Communications networks (e.g., viruses, worms, Trojan horses).

Backup Policy

Back-up procedures, ensuring that both data and software are regularly and securely backed-up, are essential to protect against the loss of that data and software and to facilitate a rapid recovery from any production server failure. This document outlines guidelines for Airbus DS Communications Hosting Center staff on backing up client data.

The data backup element of this policy applies to all Airbus DS Communications Hosting Center staff that interacts with production servers connected to the Airbus DS Communications Hosting Center network or who process or store information owned by Airbus DS Communications Hosting Center clients.

Business Continuity Policy

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

Mc
7-21-2015

Airbus DS Communications Hosting Center

This document addresses business continuity policy as it relates to Airbus DS Communications. It will guide the planning and testing of procedures to restore all facilities, systems, processes, and documentation necessary to the business operations of Airbus DS Communications in the event of a disaster.

Airbus DS Communications depends on its business systems, and especially its information processing and telecommunications systems, to provide emergency notification services to its clients. It is critical that business continuity planning take into consideration the possibility that the same disasters that can cause Airbus DS Communications' systems to be in greatest demand can also threaten our own business processes, systems, and infrastructure. These risks must be account for in Airbus DS Communications' business continuity plans.

Additionally today's distributed data processing and business applications environment expands the scope of business continuity planning and makes it more important. This increased importance arises from the possibility that systems critical to the functioning and reputation of Airbus DS Communications have become distributed outside the domain of systems backed up to offsite media.

Change Management Policy

The purpose of this document is to define policy to document, communicate and control changes to the Airbus DS Communications Hosting Center infrastructure, systems, applications, and databases while providing assistance to the change owner to ensure secure, reliable, timely, and successful changes.

The Change Management Policy and Change Control Procedures have been defined to ensure a uniform change control process, increase the reliability of the production environment, reduce time and staff requirements, and make the process of modifications and enhancements as transparent as possible to Airbus DS Communications customers. This change management policy impacts security because it ensures systems and databases are protected from unauthorized changes and properly segregates the duties of operations, development, and support staff.

Data Privacy Policy

Airbus DS Communications provides emergency notification services to clients worldwide and acknowledges the responsibility entrusted to us in managing this information and we maintain a commitment to preserve the privacy and integrity of client data. All information shared with Airbus DS Communications is subject to Airbus DS Communications' Information Sensitivity Policy and Data Security Policy, and all controls specified therein. This Data Privacy Policy governs the collection, management, and disposal of information, both emergency notification and operational, shared with Airbus DS Communications by its customers. Employees without a legitimate business need will not be granted access to customer data, nor will that data be shared with 3rd parties, unless at the request of the customer. Finally, Airbus DS Communications makes every effort to comply with all federal and state laws governing corporate and personal data privacy.

Data Security Policy

This document defines policy to secure customer data at Airbus DS Communications from first receipt and for as long as that data is managed by Airbus DS Communications, or until such data is destroyed. These measures primarily guide in controlling access to customer data and backup/recovery procedures for this data. Airbus DS Communications maintains a commitment to protect each customer's data.

Email Security Policy

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

AC
2-21-2015

Airbus DS Communications Hosting Center

The Airbus DS Communications hosting center email server is for hosting center email communications and for emergency notifications by its products. It secures internal email with enhanced anti-virus protection. Emergency email notifications shall be secured using PGP and embedded user codes. User codes are assigned to users by customers and then automatically embedded into emergency notifications sent to those users by Airbus DS Communications products. When the user replies to the email, the code is retained in the text and adds additional verification that the email came from the targeted user.

Encryption Policy

The purpose of this policy is to provide guidance on the use of encryption algorithms at Airbus DS Communications. Proven, standard algorithms such as 3DES, DES, Blowfish, RSA, RC5 and IDEA should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. Symmetric cryptosystem key lengths must be at least 128 bits. Asymmetric cryptosystem keys must be of a length that yields equivalent strength. The use of proprietary encryption algorithms is not allowed for any purpose, unless approved by Airbus DS Communications hosting center management. Airbus DS Communications will use 2048-bit SSL encryption for web interfaces and 168-bit 3DES encryption, with HMAC MD5 authentication, with VPN.

Facilities Access Control Policy

The original facility access policy has been retired due to the relocation of all production servers to the managed data facilities in Nashville, TN and Mesa, AZ. Details of the physical security aspects of these facilities is available upon request.

Information Classification & Distribution Policy

The Information Classification & Distribution Policy is intended to assist employees with classifying information into sensitivity levels. Once classified, this policy will provide guidance in the proper distribution of that information based on its sensitivity classification. It should be noted that the sensitivity level definitions were created as guidelines that must be accompanied by common sense steps to protect Airbus DS Communications's confidential information.

The information covered in these guidelines includes, but is not limited to, information stored or shared via any means, including electronic, paper, oral, and visual information. All employees should familiarize themselves with the information labeling and handling guidelines.

Network Security Policy

This document defines policy to ensure the security of the hosting center network. The hosting center network is a separate network from Airbus DS Communications corporate network. These policies intended to preserve the integrity of that network can be categorized by server, firewall, and monitoring policies.

Password Policy

Passwords are the front line of protection for user accounts, which are the gateway to systems and data. A poorly chosen password may result in the compromise of Airbus DS Communications networks, and therefore corporate and customer data. As such, all Airbus DS Communications employees and hosted clients are responsible for taking appropriate steps to select and secure their passwords as specified in Airbus DS Communications' Password Policy document. The purpose of that policy is to establish a standard for creating strong passwords, protecting these passwords, and establishing guidelines for frequently changing these passwords.

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

Page 8 of 89

AC
7-21-2015

Airbus DS Communications Hosting Center

Personnel Screening Policy

In order to create a safe and secure workplace and to ensure that Airbus DS Communications employees are qualified to perform the jobs for which the company hires them, the company will conduct pre-employment screening for all regular employees.

The Airbus DS Communications Human Resources Department shall check references and verify the educational credentials, employment histories and past performance of a finalist before it extends a final offer of employment.

When a position is designated as "security sensitive," as are all Hosting Center positions, Human Resources will obtain information on a finalist's criminal history and verification of that individual's identity.

Remote Access Policy

The purpose of this policy is to define standards for connecting to Airbus DS Communications s hosting center network from any host. These standards are designed to minimize the potential exposure to Airbus DS Communications from damages which may result from unauthorized use of Airbus DS Communications hosting center resources. Remote access is permitted by customers and hosting center employees for administrative purposes, and by customers for emergency notification activations and responses. It is especially important to secure these connections because there is no opportunity to apply physical access security controls. Remote Access Policies generally fall into three categories: authorization policies, password policies, and encryption requirements.

Security Awareness and Training Policy

The purpose of this policy is to define standards for the Airbus DS Communications Hosting Center Security Training and Awareness Program.

The Airbus DS Communications Hosting Center approach is to focus on planning, executing, and assessing training needs while integrating a common training methodology across all affected departments to optimize training effectiveness and efficiency. This policy applies to all Airbus DS Communications Hosting Center Infrastructure and Customer Support staff with access to the Hosting Center network.

Security Review and Audit Policy

The purpose of this policy is to establish review and audit requirements for all Airbus DS Communications Hosting Center critical and sensitive systems/applications and to ensure compliance with Hosting Center policies.

The Hosting Center Infrastructure Team shall ensure that all critical and sensitive systems/applications and the related infrastructure shall be evaluated as an ongoing process to improve the quality of its operations. This policy shall apply to all facilities.

Security Testing Policy

To establish the security testing requirements for Airbus DS Communications Hosting Center Infrastructure.

Security testing shall be performed on a periodic basis to ensure that information resources are adequately protected. The security testing policy applies to all systems/applications, the network and the physical infrastructure to evaluate the effectiveness of the security measures and controls implemented.

Security Violation Policy

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

bc
7-11-2015

Airbus DS Communications Hosting Center

This document defines the policy of how Airbus DS Communications will react to security violation which occurs within our hosting facilities.

These procedures apply to all Airbus DS Communications employees, contractors, and third-party entities responsible for the installation, configuration, and administration of the Airbus DS Communications Hosting Center network. No individual who supports these entities or processes shall be exempt from this policy.

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

hc
7-21-2015

Airbus DS Communications Hosting Center

Server Security Policy

The purpose of this policy is to establish standards for the base configuration of hosted servers and workstations that connect to them. Effective implementation of this policy will minimize unauthorized access to hosted systems, the applications and data they host, and Airbus DS Communications proprietary information and technology. This policy establishes standards for server configurations, access-controls, and server monitoring.

Service Problem and Critical Incident Management Policy

This Policy prescribes how service problems and requests for assistance are managed by Airbus DS Communications Hosting Infrastructure. It includes Procedures for allocating priorities to problems, handling routine problems and requests, and for managing critical incidents.

The Policy covers all service problems and requests for assistance received by Hosting Center staff for all facilities. This may include service interruptions notified by system monitoring alerts, and Customer Support Staff responding to support requests by clients/users of Hosting Center facilities. All service problems will be recorded into the call tracking software. Some routine requests not affecting any specific clients may not be recorded into the call tracking software, but will be recorded for statistical analysis.

Software Maintenance Policy

This document defines policy for performing routine maintenance of hosting center systems. Due to the need for O/S updates, application upgrades, Airbus DS Communications product hot fixes, and the day-to-day growth of system files all systems require a maintenance plan. These maintenance activities should be scheduled to minimize customer interference, downtime, and emergency system restore time.

These procedures apply to all hosting center systems hosting customer products and implemented in conjunction with the Change Management Policy and Change Control Procedures. No individual who supports the operations of Airbus DS Communications shall be exempt from this policy.

System Monitoring Policy

The purpose of the Monitoring Policy is to ensure that Proactive infrastructure health and performance monitoring controls are in place. Airbus DS Communications uses system and software monitors to ensure the health and performance of all hosted customer systems. Monitors provide trend information that can identify problems long before they impact the function of our hosted systems. Monitoring our systems also ensures that we meet our system uptime requirements. In the event of a monitor reporting data out of limits for normal activity, email and pager notifications are sent to hosting center staff. These notifications are resent until resolution of the problem.

Systems Access Control Policy

This policy defines system access control policies for Airbus DS Communications hosted systems. System access is controlled by applying policies to the server, applications, and network. This policy is accomplished by applying the access control policies contained within the Network Security Policy, Server Security Policy, Remote Access Policy, and Password Policy.

Virtual Private Network Policy

The purpose of this policy is to provide guidelines for Remote Access IPsec or SSL Based Virtual Private Network (VPN) connections to the Airbus DS Communications Hosting Center network.

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

hc
7-21-2014

Airbus DS Communications Hosting Center

This policy applies to all Airbus DS Communications Hosting Center employees, contractors, consultants, temporaries, customers and other workers including all personnel affiliated with third parties utilizing VPN to access the Airbus DS Communications Hosting Center network.

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

Re
7-21-2015

Security Procedures Summary

1.0 Purpose

This document is a highlighted list of procedures used to secure Airbus DS Communications hosted customer systems, data, and communications (voice and data). This listing is intended as a summary of procedures Airbus DS Communications has in place, but by no means is intended to be an exhaustive list.

2.0 Scope

These procedures apply to all Airbus DS Communications employees, contractors, and third-party entities responsible for the installation, configuration, administration, and transportation of hosted customer systems and data. No individual who supports these entities or processes is exempt from these procedures.

3.0 Policy

The following are security related topics addressed by Airbus DS Communications to provide a comprehensive security strategy for customer-hosted systems, data, and communications. For an in-depth review of each of these policies, see the associated section by the same name within this document. One security related policy that is a footnote to each of the following security topics is the *Employee/Contractor Termination Policy* which requires all physical and system access be immediately terminated upon termination of service by an employee or contractor.

Anti-Virus Protection Policy

- All Airbus DS Communications PC-based Hosting Center servers and workstations have Airbus DS Communications standard, supported anti-virus software installed and scheduled to run at least daily.
- Anti-virus software automatically applies critical updates at least weekly.
- Virus-infected computers are removed immediately from the network until they are cleansed and certified virus-free.

Backup Policy

- A full systems backup will be performed weekly. Weekly backups will be saved for a full month.
- The last weekly backup of the month will be saved as a monthly backup. The other weekly backup media will be recycled for other uses or destroyed.
- Monthly backups will be saved for one year, at which time the media will be recycled or destroyed.
- Incremental backups will be performed daily. Incremental backups will be retained for two weeks, at which time the media will be recycled or destroyed.
- All backups will be stored in a secure, off-site location. Proper environment controls, temperature, humidity and fire protection, shall be maintained at the storage location.
- All backup media that is not re-usable shall be thoroughly destroyed in an approved manner. Backup media that is used for other purposes shall be thoroughly erased.
- Periodic tests of the backups will be performed to determine if files can be restored.

Change Management Policy

- Where possible, changes to hosting center infrastructure, systems, and databases will undergo quality assurance testing and certification.

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

RC
7-21-2015

Airbus DS Communications Hosting Center

- Changes to hosting center infrastructure can only be executed by the Hosting Center Infrastructure Team.
- All non-routine hosting center infrastructure, systems, and database changes must be approved by and coordinated with the customers impacted by the change. Where possible, a customer is given a minimum seven days advanced notice.

Change Management Procedure

- Document the reason for change
- Identify who is requesting the change
- Formalize who will make the change
- Define how the change will be made
- Document back out procedures should the need arise
- Assess the risk of failure and impact of the change
- Aid in communicating with those affected by the change
- Identify disaster recovery considerations
- Identify conflicts between multiple changes
- Enhance management's awareness of all of the above.

Customer Support Procedures

- Calls are routed to a dedicated ACD at 615.550.0200.
- If a customer calls and receives a recording it means that all Support Desk analysts are at that moment busy assisting other customers.
- The caller will be transferred to the operator.
- If the caller is experiencing an emergency they may request that the operator page a support manager to provide assistance.
- If the call is not an emergency, they will be put into the support voice mail where they should leave their name, company name and ID, telephone number and a brief description of the reason for the call. Messages are checked frequently and calls are returned in the order in which they are received, but always within four (4) hours.
- Callers will be given a ticket ID# to use when calling again about the same issue.
- If the customer is experiencing an emergency outside Normal Business Hours (defined as 8am – 5pm CST; Monday through Friday, excluding holidays) they should call the support number at 615.550.0200.
- The call will be routed to a live operator where the customer should leave a clear voice message with their name, company name and ID, telephone number and a brief description of the reason for the call.
- The on-call technical analyst will be paged and will return the call within an hour.

Airbus DS Communications Customer Support outside NBH ensures a customer support representative, infrastructure administrator, and infrastructure technician are on-call. Standard business hours, in conjunction with Airbus DS Communications' after-hours program, provide customers 24x7 emergency support. Airbus DS Communications Customer Support After-Hours personnel can be directly contacted by the customer, automated systems monitoring notifications, and other on-call personnel.

Data Privacy Policy

- Airbus DS Communications provides emergency notification services to clients worldwide and acknowledges the responsibility entrusted to us in managing this information.

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

RC
7-11-2015

Airbus DS Communications Hosting Center

- We maintain a commitment to preserve the privacy and integrity of client data. All information shared with Airbus DS Communications is subject to Airbus DS Communications' *Information Sensitivity Policy* and *Data Security Policy*, and all controls specified therein.
- This *Data Privacy Policy* governs the collection, management, and disposal of information, both emergency notification and operational, shared with Airbus DS Communications by its customers.
- Employees without a legitimate business need will not be granted access to customer data, nor will that data be shared with 3rd parties, unless at the request of the customer.
- Finally, Airbus DS Communications makes every effort to comply with all federal and state laws governing corporate and personal data privacy."

Data Security Policy

- All customer data is backed up to tape, encrypted, and stored offsite where it is retained for at least one year.
- Customer data is backed up in a manner that permits full recovery to any specified date. These recoveries include the ability to recover system configuration settings, such as registry settings.
- All sensitive customer data is stored on secured hosting center production servers.
- Airbus DS Communications provides a fax machine in a secured location for transmitting sensitive data.
- Customer data is only transmitted across secure communications media (SSL, SFTP, etc), unless explicitly requested otherwise by the customer.
- A separation of duties exists between individuals who authorize data access and personnel who enable data access.

Email Security Policy

- The Airbus DS Communications hosting center email server utilizes industry standard anti-virus protection and applies critical updates daily.
- Emergency email notifications are secured using embedded user codes used to further validate a user's response.

Employee/Contractor Termination Procedure

- Confirm the individual's building access card has been recovered
- If applicable, recover any support pagers in person's possession
- Request Information Technology disable person's corporate LAN account, which also disables their Virtual Private Network (VPN) login
- Request the Information Technology disable person's corporate Exchange email access
- If applicable, disable person's departmental network accounts
- If applicable, disable person's VPN account on the Airbus DS Communications network
- If applicable, contact off-site data facilities to remove access authorization

Encryption Policy

- 2048 bits SSL encryption on all web interfaces; SSL signatures shall be used with sha1RSA, 128 bit encryption, Public Key. HTTPS shall be 2048 bit security. Data transferred to and from servers is transferred using Digital Signature, Key Encipherment, and Data Encipherment.
- Data will be encrypted before being stored offsite.
- Copies of public key are kept offline located in a fireproof safe on encrypted media.
- Each VPN Tunnel uses 168 bit 3DES encryption and HMAC MD5 authentication is used to verify integrity.

Facilities Access Control Policy

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

nc
7-21-20

Airbus DS Communications Hosting Center

- The original facility access policy has been retired due to the relocation of all production servers to the managed data facilities in Nashville, TN and Mesa, AZ. Details of the physical security aspects of these facilities is available upon request.

Information Classification & Distribution Procedures

- The Information Classification & Distribution Procedures is intended to assist employees with classifying information into one of three sensitivity levels.
- Information's classification guides employees in the proper storage, distribution, management, and disposal of information.

Network Security Policy

- Airbus DS Communications' Hosting infrastructure is independent of the corporate network. This ensures corporate failures are isolated from customer systems.
- Each customer system is protected by a dedicated firewall to ensure that any system that might be compromised is isolated from all other Airbus DS Communications customers.
- Firewalls are configured to report unauthorized access to Airbus DS Communications systems. Any breach of security or unusual attack on a client's server is reported to that client.
- Firewalls translate internal addresses to mask the actual name and address of internal machines communicating outside Airbus DS Communications.
- SSL (HTTPS) with 2048 bit encryption is required on all Airbus DS Communications web servers.

Password Policy

- All system passwords are changed every 90 days.
- All user-level passwords are changed every 180 days.
- Passwords must be at least eight characters in length and contain both numeric and alpha characters.

Personnel Screening Policy

- Airbus DS Communications performs credit, criminal, workers compensation, background, previous employment reference, and personal reference checks for all employees and contractors prior to granting unescorted access to hosting center systems or data.

Remote Access Policy

- Remote access is only permitted by hosting center employees for administrative purposes and by customers for emergency notification activations and responses.
- Remote access is validated through windows authentication, application usernames and passwords, scenario ids, and roster member user ids.
- Files must be exchanged using Secure FTP, unless specifically requested otherwise by the client.
- Remote server-to-server connections are secured through SSL certifications.
- Remote access users have their activities logged. These logs are monitored with alerts and inspected as needed. Logs are backed up offsite and retained for at least one year.

Security Awareness and Training Policy

- Development and maintenance of a Hosting Center security training and awareness program for all Hosting Infrastructure and Customer Support personnel is required in accordance with this policy.

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

Ac
~ ~ ~ ~ ~

Airbus DS Communications Hosting Center

- Training programs shall be tailored to a user's need-to-know for secure operation or use of the Hosting Center network and related systems.
- Primary security areas, at a minimum, shall be addressed during training:
- Security training and awareness can be accomplished using multiple delivery methods:
- Hosting Center awareness and training is required for all authorized users before they are granted access to the Hosting Center Network or associated systems. Refresher training shall be conducted annually and when major policy changes occur (e.g., a new policy is implemented).
- A documented process for tracking and reporting training provided to all users, including the name of the person attending, instruction format, dates of attendance, and shall be recorded to ensure compliance with requirements.

Security Review and Audit Policy

- System Activity Reviews
- Formal Audit Process
- Regular Audit/Review
- System Audit Logging
- Fault Logging
- Audit Trail Documentation
- Restrict access to Audit Logs and Audit Trail Data

Security Testing Policy

- Developing a Security Test Strategy.
- General Security Test and Evaluation Process
- Scheduling Security Tests.
- Types of Security Tests.
 - a. Network Mapping
 - b. Vulnerability Scanning Penetration Testing
 - c. File Integrity Checkers
 - d. Anti-Virus and Malicious Code Detection
 - e. Physical Access Testing
- Log Reviews.
- Recommending Security Enhancements.

Security Violation Policy

- Airbus DS Communications monitors its network infrastructure for security breaches using firewall, IDC, and server level tracking.
- If a suspected breach is detected by an automated process or infrastructure technician, the Hosting Center Manager is contacted immediately.
- The Hosting Center Manager will determine whether there has been a breach or there is cause for further investigation and, if so, will then notify the Vice President of Hosted Services.
- In the event that a Security breach is confirmed and Airbus DS Communications personnel have reason to believe that customer data may have been compromised, Airbus DS Communications will bring in an independent third party to investigate the validity and extent of the incident.
- Actions will be taken immediately to isolate and contain any network segment or server that has been compromised.
- At the earliest opportunity, the Hosting Center Manager or his staff will notify Customer support with details of any systems that have been exposed to the threat and any customers that might have been affected.

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

hc
2014

Airbus DS Communications Hosting Center

- Immediately following a security incident a security review meeting will be called by the Vice President of Hosted Services to review actions taken during the event and discuss potential changes to policies and procedures.

Server Security Policy

- Unnecessary server services and applications are either not installed or disabled.
- User access to servers and applications is logged, monitored, and reviewed as needed. Logs are stored offsite and retained for at least one year.
- Microsoft security updates are applied to all servers on a weekly basis.
- All hosted servers are monitored for health checks 24x7. Threshold violations are automatically sent out to on-call personnel in the form of pages and emails. These alerts are automatically escalated until a response is received.
- Trust relationships between hosted servers are not permitted.
- All system access for hosting center production servers must be approved by Infrastructure Management.
- Only the Infrastructure organization has access to system administrative tools unless otherwise requested by the customer.
- A separation of duties exists between individuals who authorize system access and personnel who enable system access.

Service Problem and Incident Management Policy

- Problems are escalated if they are not resolved within the following timeframes:
 - a. Priority 1: 30 minutes to Senior Hosting Infrastructure technician
 - b. Priority 2: 2 hours to Senior Hosting Infrastructure technician
 - c. Priority 3: 1 working days to Hosting Infrastructure Manager for analysis and action
 - d. Priority 4: 5 working days to Hosting Infrastructure Manager for analysis and action problems escalated to the Hosting Infrastructure Manager will be managed according to the 'Critical Incident Procedure'.

Prioritizing Service Problems Procedure

- How many users are affected, and what is the impact to the business?
- Can the problem wait till the next working day?
- Is there an alternative way to carry out the work (i.e. manual process)?
- What type of work is being affected, i.e. production or testing?
- Is the production limitation holding up the clients business need, or can they continue working without this service?
- How urgent or important is this activation?
- Will a customer contact be available assist in problem resolution?
- Will access to replacement hardware/equipment be available if required?

Critical Incident Management Procedure

- Receiving/detecting high priority problems
- Performing initial assessment
- Allocating the problem to a Support Section
- Notify the Hosting Infrastructure Manager
- If the problem does not look resolvable within the approved timeframes, escalate
- Liaising with Hosting Infrastructure Manager
- Client communications
- Senior Management communications

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

Page 18 of 89

Mc
7-21-20

Airbus DS Communications Hosting Center

- Verify correct resources have been allocated to the problem
- Initial Contingency Actions
- Ascertain if Vendor support is needed
- Ongoing problem resolution
- Service restoration and review

Software Maintenance Policy

Routine Maintenance:

- Windows updates
- Application upgrades
- Defrag
- Log file maintenance Review
- Empty Window's recycle bin.
- Reboot server
- Logout of server
- Verify the system is live again.

Non-Routine Maintenance:

- Hot Fixes – periodically Airbus DS Communications releases hot fixes for its products. There should be a coordinated plan for applying these updates.

System Monitoring Policy

- CPU Utilization Monitor
- Disk Space Monitor
- Memory Monitor
- Network Monitor
- Service Monitor
- URL Monitor
- FTP Monitor
- Ping Monitor
- Operator Monitoring

Virtual Private Network Policy (VPN)

- It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to Airbus DS Communications Hosting Center networks.
 - VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong pass phrase.
 - When actively connected to the Hosting Center network, VPN will force all traffic to and from the PC over the VPN tunnel; all other traffic will be dropped.
 - Dual (split) tunneling is NOT permitted; only one network connection is allowed.
 - VPN gateways will be set up and managed by Airbus DS Communications infrastructure operational groups.
 - All computers connected to Airbus DS Communications Hosting Center networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard (provide URL to this software); this includes personal computers.
 - VPN users will be automatically disconnected from Airbus DS Communications Hosting Center's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
 - The VPN concentrator is limited to an absolute connection time of 24 hours with the exception of site-to-site VPN connections between facilities.
-

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

hc
- 11-2014

Anti-Virus Policy

1.0 Purpose

To establish requirements which must be met by all computers connected to Airbus DS Communications Hosting Center networks to ensure effective virus detection and prevention.

2.0 Scope

This policy applies to all Airbus DS Communications Hosting Center computers that are PC-based or utilize PC-file directory sharing. This includes, but is not limited to, desktop computers, laptop computers, file/ftp/tftp/proxy servers, and any PC based lab equipment such as traffic generators.

3.0 Policy

All Airbus DS Communications PC-based Hosting Center computers must have Airbus DS Communications standard, supported anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus pattern files must apply critical updates within two weeks of their release. Virus-infected computers must be removed from the network until they are verified as virus-free. Infrastructure Technicians are responsible for creating procedures that ensure anti-virus software is run at regular intervals, and computers are verified as virus-free. Any activities with the intention to create and/or distribute malicious programs into Airbus DS Communications networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Guidelines on Anti-Virus Process

Recommended processes to prevent virus problems:

- 1) All Airbus DS Communications PC-based Hosting Center computers must have Airbus DS Communications standard, supported anti-virus software installed.
 - 2) Always run the corporate standard, supported anti-virus software is available from the Hosting center download site. Download and run the current version; download and install anti-virus software updates as they become available.
 - 3) NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
 - 4) Delete spam, chain, and other junk email without forwarding
 - 5) Never download files from unknown or suspicious sources.
 - 6) Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
 - 7) Always scan a floppy diskette from an unknown source for viruses before using it.
 - 8) Back-up critical data and system configurations on a regular basis and store the data in a safe place.
 - 9) If lab testing conflicts with anti-virus software, run the anti-virus utility to ensure a clean machine, disable the software, then run the lab test. After the lab test, enable the anti-virus software. When the anti-virus software is disabled, do not run any applications that could transfer a virus, e.g., email or file sharing.
 - 10) New viruses are discovered almost every day. Periodically check the Lab Anti-Virus Policy and this Recommended Processes list for updates.
-

Backup Policy

1.0 Purpose

Back-up procedures, ensuring that both data and software are regularly and securely backed-up, are essential to protect against the loss of that data and software and to facilitate a rapid recovery from any production server failure. This document outlines guidelines for Airbus DS Communications Hosting Center staff on backing up client data.

2.0 Scope

The data backup element of this policy applies to all Airbus DS Communications Hosting Center staff that interacts with production servers connected to the Airbus DS Communications Hosting Center network or who process or store information owned by Airbus DS Communications Hosting Center clients.

3.0 Policy

Airbus DS Communications requires that computer systems maintained by Hosting Center personnel are to be backed up periodically and that the backup media is stored in a secure off-site location. The purpose of the systems backup is to provide a means to: (1) restore the integrity of the computer systems in the event of a hardware/software failure or physical disaster, and (2) provide a measure of protection against human error or the inadvertent deletion of important files. The systems backups will consist of regular full and incremental backups.

Systems backups will be performed on a regular schedule as determined by the Hosting Center Infrastructure group. Backups will be stored in a secure off-site location based on the schedule listed below.

4.0 Procedures

This policy provides guidelines for establishing backup procedures. Exceptions to the standard procedure are permitted when justified. All exceptions must be fully documented. The standard procedure for systems backup is as follows:

- 1) A full systems backup will be performed nightly. Nightly backups are retained online for 7 days and then offsite for 30 days.
- 2) Incremental database backups will be performed daily. Incremental backups will be retained for locally for 3 days and then deleted.
- 3) All backups will be stored in a secure, off-site location. Proper environment controls, temperature, humidity and fire protection, shall be maintained at the storage location.
- 4) All backup media that is not re-usable shall be thoroughly destroyed in an approved manner. Backup media that is used for other purposes shall be thoroughly erased.
- 5) Periodic tests of the backups will be performed to determine if files can be restored.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

Mc
7-11-14

Business Continuity Policy

1.0 Purpose

This document addresses business continuity policy as it relates to Airbus DS Communications. It will guide the planning and testing of procedures to restore all facilities, systems, processes, and documentation necessary to the business operations of Airbus DS Communications in the event of a disaster. For the remainder of this document, "business systems" will refer to these facilities, systems, processes, and documentation. Business systems will be identified, categorized, and prioritized for the purpose of building business resumption plans (BRPs) and contingency plans (CPs).

Airbus DS Communications depends on its business systems, and especially its information processing and telecommunications systems, to provide emergency notification services to its clients. It is critical that business continuity planning take into consideration the possibility that the same disasters that can cause Airbus DS Communications' systems to be in greatest demand can also threaten our own business processes, systems, and infrastructure. These risks must be account for in Airbus DS Communications' business continuity plans.

Additionally today's distributed data processing and business applications environment expands the scope of business continuity planning and makes it more important. This increased importance arises from the possibility that systems critical to the functioning and reputation of Airbus DS Communications have become distributed outside the domain of systems backed up to offsite media.

2.0 Scope

This policy is applicable to Franklin, TN and Mesa, AZ facilities, and all employees and contracted agents who support Airbus DS Communications business systems. No employee, contractor, or third party is exempt from this policy.

3.0 Policy Goals

For the purposes of business continuity planning, Airbus DS Communications' business will be organized into key subject areas. Subject area teams, members of an overseeing Business Continuity Management Team (see below), will be responsible for creating subject area business resumption plans. The following subject areas and goals, though not intended to be exhaustive, are set forth to guide the development of subject area business resumption plans.

Hosting Center:

- a. Minimize disruptions of service to Airbus DS Communications customers relying on hosted systems
- b. Ensure quick resumption of 24x7 support to hosting center customers after a disaster
- c. Limit the impact of Hosting Center disruptions on Airbus DS Communications' reputation
- d. Limit corporate financial loss from hosting center disruptions
- e. Minimize disruptions of telecommunications services to hosting center customers
- f. Ensure the timely resumption of critical systems and services at the earliest possible time in the most cost effective manner

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

nc
7-21-20

Airbus DS Communications Hosting Center

- g. Ensure data as well as system, firewall & switch configurations are backed up offsite and detailed plans exist for their quick restoration
- h. Ensure all network and system diagrams, policies and procedures, customer configurations, customer and vendor contracts, and emergency contacts are stored offsite and available for quick retrieval
- i. Contract critical vendors for specified service level agreements during a disaster
- j. Ensure the security of systems and data during business systems restoration

Network Operations Center:

- a. Minimize disruptions of service to Airbus DS Communications personnel who rely on corporate applications for business and communication functions
- b. Minimize disruptions of telecommunications services to hosting center customers
- c. Ensure the timely resumption of critical systems and services at the earliest possible time in the most cost effective manner
- d. Ensure data as well as system, firewall & switch configurations are backed up offsite and detailed plans exist for their quick restoration
- e. Ensure all network and system diagrams, corporate systems and network configurations, policies and procedures, vendor contracts, and emergency contacts are stored offsite and available for quick retrieval
- f. Contract critical vendors for service level agreements during a disaster
- g. Ensure the security of systems and data during business systems restoration

Facilities:

- a. Ensure utilities are available to support BRPs (power, water, etc)
- b. Ensure building security in the event of a disaster
- c. Ensure office equipment are available to support BRPs

Financials:

- a. Arrange finances to support BRPs
- b. Arrange proper insurance coverage for disasters
- c. Ensure duplicate copies of financial contracts, forms, policies and procedures, and emergency contacts necessary to conduct Airbus DS Communications financials are stored offsite and available for quick retrieval
- d. Ensure financial systems and data are stored offsite and available for quick retrieval

Human Resources:

- a. Ensure personnel files are backed up offsite
- b. Ensure contractor and vendor agreements are backed up offsite
- c. Responsible for temporary personnel necessary to support BRPs

Customer Service:

- a. Ensure quick resumption of 8-to-5 support to onsite customers after a disaster
- b. Ensure duplicate copies of contracts, forms, policies and procedures, and emergency contacts necessary to conduct customer service are stored offsite and available for quick retrieval

Development:

- a. Ensure product source code is backed up offsite and plans exist for its quick retrieval

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

20

Airbus DS Communications Hosting Center

- b. Ensure technical documentation is backed up offsite and plans exist for its retrieval
- c. Ensure developers have necessary tools (workstations, software, etc) to support products after a disaster

Installations:

- a. Ensure facilities exist to stage and test new installations during a prolonged facilities disruption
- b. Ensure duplicate copies of customer configurations, forms, policies and procedures, and emergency contacts necessary to conduct installations are stored offsite and available for quick retrieval

Training:

- a. Ensure electronic copies of training materials are stored offsite
- b. Ensure customers can receive training during a prolonged training facility disruption

Sales:

- a. Ensure duplicate copies of sales contracts, customer information, forms, policies and procedures, and emergency contacts necessary to conduct sales are stored offsite and available for quick retrieval

Purchasing:

- a. Ensure purchases can be made to support BRPs during a disaster
- b. Ensure contracts exist with vendors supplying critical BRP equipment
- c. Ensure vendor contracts, forms, policies and procedures, and emergency contacts necessary to purchasing are stored offsite and available for quick retrieval

4.0 Business Resumption Plans

Once critical business systems have been identified, Business Resumption Plans (BRPs) shall be developed and tested for timely restoration of these business systems. Copies of the BRPs shall be accessible from any off-site location. Key personnel should know the exact location of the BRPs and be familiar with how to access and execute these plans. BRPs for critical and essential systems shall contain the following:

- a. Clarification of what constitutes a disruption for which the specific BRP needs to be implemented.
- b. Maximum acceptable downtimes that can be incurred.
- c. Who from each subject area works with the Executive Coordinating Officer to determine whether an incident is classified as a business disruption, what level of disruption has occurred and to what degree the plan needs to be implemented.
- d. Which staff is involved in the business resumption effort.
- e. What are the resumption team member responsibilities and how will the non-availability of certain key team members be addressed. Step-by-step, definitive procedures for each team member shall be developed. Plans for cross training on duties should also be formulated. Pre-planned processes and trained personnel will significantly reduce the cost and time necessary to achieve full recovery and resume normal business operations.

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

Mc
7-21-20

Airbus DS Communications Hosting Center

- f. An emergency call list for key personnel shall be developed. Contact names, phone lists and initiation procedures are updated as needed.
- g. The location of the BRP coordination site(s), if needed.
- h. What information about the disruption shall be made public and how this information will be disseminated.
- i. An inventory of all critical resources necessary to resume operations including, but not limited to: systems, applications, communication requirements (telecommunications, network, internet, modems, etc.), facility requirements (A/C, heat, power, raised floor, cabling, communications, square footage, personnel, etc), hardware, data backup availability, vendor support, staff, documentation, security, office equipment, funding, and transportation.
- j. Data back-up locations, schedules, and recovery procedures to include system restore procedures.
- k. Contracted or agreed upon alternate facilities/operating sites. Copies of contracts should be kept at an off-site location.
- l. Information regarding the type and level of vendor support required, available and contracted.
- m. The off-site location of duplicate documentation (BRP, system/application manuals, contracts, procedure manuals, policies and procedures, etc.), supplies, and forms.
- n. A schedule for BRP testing. BRPs shall be tested at least annually using various testing approaches (e.g., structured walk-through; checklists; simulations; parallel testing; and full-interruption testing). Tests should be carefully planned to minimize disruption to normal operations and should address partial and full disruptions of various types. After each test exercise, results should be thoroughly reviewed for flaws, omissions, and overlaps in the business resumption procedures. Test results should be made available to the Business Continuity Management Team.

5.0 Continuity Plans

Contingency plans are temporary business systems that meet minimum business system requirements but can be implemented quickly to support the business while BRPs are executed. A contingency plan might be a paper payroll system used for two days while servers are procured to restore an electronic payroll system, or a pool of cell phones used to provide customer support while a temporary service center is readied for calls. Not all BRPs need continuity plans, nor is it always practical or cost effective to have them.

6.0 Risk Assessments

Each Airbus DS Communications organization must conduct an annual risk assessment to identify risks to their critical processes, products, and services. Each risk will be categorized with mitigation and recovery plans documented. These efforts will be the responsibility of the Business Restoration Teams.

7.0 Business Continuity Management Team

Planning and executing a business continuity plan requires a team representing cross-sectors of the company business. In the event of a disaster, the BCMT provides general support, while the Support Teams manage the coordination of resources and tasks essential to restoring and operating the various business systems. This section defines the roles and responsibilities that compose the BCMT.

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

AC
7-21-2014

Airbus DS Communications Hosting Center

Executive Coordinating Officer – Coordinates the BCMT by coordinating the operational, management, and support teams. This person is also responsible for maintaining and testing the company's BCP and, in the event of an incident, for declaring a disaster and specifying which BRPs shall be executed.

Hosting Center Coordinator – coordinates support for primary and backup hosted systems and works closely with 3rd party facility managers representing each critical Airbus DS Communications facility.

Telecommunications Coordinator – coordinates support for the telecommunications for Airbus DS Communications corporate, and both primary and backup hosting centers.

Corporate Network Coordinator – coordinates support for Airbus DS Communications' corporate network.

Security Officer – provides for physical and emergency support for business systems and ensures notification mechanisms exist. During a disaster, the Security Officer ensures the security of business systems during execution of the BRPs.

Insurance & Legal Representative – provides liaison to insurance carriers and claims adjusters.

Airbus DS Communications Public Relations Coordinator – is responsible for all Airbus DS Communications communication with the public and media during a disaster.

Human Resource Coordinator – provides support to personnel during a disaster.

Comptroller – coordinates the finances to support the disaster recovery efforts.

Business Restoration Teams – coordinates the planning and execution of individual BRPs.

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

nc
7-21-20

Change Management Policy

1.0 Purpose

The purpose of this document is to define the policy to document, communicate and control changes to the Airbus DS Communications Hosting Center (infrastructure, systems, applications, and databases) while providing assistance to the change owner to help ensure secure, reliable, timely, and successful changes.

The Change Management Policy has been defined to ensure a uniform change control process, increase the reliability of the production environment, reduce time and staff requirements, and make the process of modifications and enhancements as transparent as possible to Airbus DS Communications customers. This change management policy is designed to ensure Hosting Center infrastructure, software, and databases are protected from unauthorized changes and there is a proper segregation of duties between operations, development, and support staff.

2.0 Scope

This policy is applicable to all employees and contracted agents who perform functions affecting the development or installation of Hosting Center infrastructure, application, or database changes. No employee, contractor, or third party is exempt from this policy. Change management policy must be applied whenever the Hosting Center infrastructure, systems, applications, databases, or data—regardless of the size or presumed impact of that modification—are changed. Data changes made either by customers using standard Airbus DS Communications application interfaces or Airbus DS Communications employees using standard administrative processes are exempt from this policy.

3.0 Policy

All changes to the Hosting Center infrastructure, systems, and databases must observe the following guidelines:

- 1) Changes to Hosting Center infrastructure can only be executed by the Hosting Center Infrastructure team
- 2) All non-routine Hosting Center infrastructure, systems, and database changes must be approved by and coordinated with the customers impacted by the change
- 3) All customers of shared systems must be notified of changes and given a minimum of 5 business days notice for non-emergency changes. Shared systems do not require the approval of all customers.
- 4) All Hosting Center infrastructure, systems, and database changes must be tracked and available for reporting by the Change Manager (see *Change Management Procedures*).

Changes and/or modifications can be subdivided into four categories. Depending on impact to users and other systems, a change is considered to be one of the following:

- 1) Application Enhancements
- 2) Application customizations
- 3) Systems and software upgrades
- 4) Infrastructure enhancements and upgrades

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

RC
7-21-2014

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

AC
7-21-2014

Change Management Procedure

1.0 Procedure Description

This section presents the concept of change management and control within the Airbus DS Communications Hosting Center computing environment. It describes: the reasons and objectives for the system and general flow of the system.

Reasons for Change Management

Our mission is to provide clients with notification services in a reliable and consistent manner that they can count on time after time. Changes to the production environment allow opportunities for errors that may disrupt our ability to provide high quality services to the clients. Managing those changes can help reduce the introduction of errors. As a result, this procedure is a process to manage changes within the Airbus DS Communications Hosting Center and its potential impact to the services provided.

Change Management will:

- 1) Document the reason for change
- 2) Identify who is requesting the change
- 3) Formalize who will make the change
- 4) Define how the change will be made
- 5) Document back out procedures should the need arise
- 6) Assess the risk of failure and impact of the change
- 7) Aid in communicating with those affected by the change
- 8) Identify disaster recovery considerations
- 9) Identify conflicts between multiple changes
- 10) Enhance management's awareness of all of the above.

A formal control process is necessary to bring change plans together in a forum that is conducive to effectively disseminating information to those who are potentially affected by a change. If done consistently and conscientiously, this process can ensure that changes are implemented in a timely fashion with little or no adverse impact on the services.

Change Management provides a means by which a historical trail of changes made to the system can be kept. This becomes valuable when the relationships between system failures and/or performance problems must be correlated and analyzed.

2.0 Change Management Process

Change Management is a vehicle for the authors of change to communicate their change implementation methodology to management, implementers, and clients. The process is intended to communicate both planning and implementation information.

3.0 Objectives

Specific objectives of change management are to maintain and improve system reliability; availability; serviceability and functionality.

4.0 Scope

This process applies to the following areas:

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

Re
7-11-2015

Airbus DS Communications Hosting Center

- 1) Hardware (Servers)
- 2) System Software (MS Windows OS, MS SQL, etc.)
- 3) Major Application Software updates (Frontwave, Communicator!, Communicator! NXT)
- 4) 3rd Party Tools (Norton's Anti-virus, Tivoli Backup, etc.)
- 5) Telecommunications (circuits)
- 6) Firewalls
- 7) Network (LAN, WAN, routers, servers, software delivery, etc)
- 8) External Factors

Specific change tasks associated with the above areas are will be identified on a case by case basis. The scope of changes managed by this process may broaden or contract as Hosting Center Infrastructure and Support deems necessary i.e., a particular type of routine change is developing an unacceptable failure pattern or that a controlled change is becoming sufficiently routine that change management no longer appears necessary.

5.0 Overview of the System

The Change Management process is comprised of six steps

- 1) Request
- 2) Planning
- 3) Approval
- 4) Schedule
- 5) Implementation
- 6) Review

In the request process, Hosting Center Infrastructure or Support personnel identify the desired change either as a function of application updates, technology changes, or client request, documents the specifics of the change, and submits to their department management for preliminary approval. All implemented changes must be recorded and tracked via the Help Desk System.

The department management will:

- Review the request for compliance to all testing, implementation, documentation, back out requirements, Disaster Recovery impact, and automation impact.
- Assess the reasonableness of the level assigned by the author based on their knowledge of the risk, impact, and history of similar changes; and assess the requirement for inter-department signatures.
- Authorize the request.
- Assign a Change Control Coordinator

The Change Control Coordinator will:

- Review the request for compliance to change management procedures
- Add the request to the schedule for change activity

The planning step lays out the specific tasks, sequences and responsibilities that must be completed for a successful change. Prerequisites and dependencies are identified and specific times are also indicated where tight coordination is necessary.

The approval process is intended to verify that all of the steps defined in the request process have been carried out and is appropriate in view of the risk and impact to the organization.

Re
- 11-10-14

Airbus DS Communications Hosting Center

In the schedule process, all approved changes are scheduled on a master activity schedule to enable all effected resources to be aware of the activities planned for the production environment. It also allows conflicts of resources and major impacts to be reviewed and revised, when necessary.

The implementation process establishes a mechanism in which changes can be applied in an effective, high-quality manner, and enables the change to be entirely removed if necessary without adversely impacting the system's ability to perform in the same manner as before the change.

The review process assesses the successful implementation of the change. Was the change completed on time? Completed correctly? What if any problems were encountered? What processes and/or procedures may require modification to ensure successful completion in the future?

6.0 The Change Approval Team (CAT)

The Team will be comprised of members of the following areas:

- VP Hosted Services
- VP Customer Support
- VP Product Development

The individuals selected to sit on CAT have been selected for their in-depth perspective and broad knowledge of the areas they represent as well as their appreciation for other functional areas involved. This degree of participation is necessary for making objective decisions on the most significant changes affecting the organization.

It is important to separate the change requesters from the change approvers in order to avoid natural conflicts.

If a Board member delegates their duties to a substitute, that substitute must be able to answer all questions regarding upcoming changes, as well as those that were scheduled for the prior week.

7.0 Change Review Meetings

Change review meetings are held as needed.

The following types of changes will be reviewed during the change review meeting:

- Baseline Configurations
- Scheduled Application Releases
- Emergency Fixes
- Hardware Changes
- Infrastructure Modifications

The Change Approval Team meets on an as needed basis to go through the final approval process for upcoming changes. The standard list of changes for this meeting includes but is not limited to:

- 1) Release Migrations
- 2) Tools Upgrades
- 3) Environment Setup for Migrations
- 4) Environment Setup for Tools
- 5) 3rd Party Upgrades
- 6) Configuration Changes
- 7) Hardware Changes

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

AC
7-11-10

Airbus DS Communications Hosting Center

The recommended change schedule, which is to be used at the CAT meeting, should be produced in sufficient time prior to the meeting to allow the Team members an opportunity to review information with their respective staff for comments and recommendations. It is during this process that much of the technical assessment or behind the scenes activity takes place. Sufficient lead time will help ensure that all necessary coordination among the various parties involved with the change can be accomplished before the request is approved.

Once the Team has approved, disapproved, or suspended a change, the change schedule will be updated to reflect the new status. That information is then communicated to the requester and to the interested parties. If the change is approved, the requester may proceed with the change implementation on the schedule documented in the approved Change Request. If the change is disapproved or suspended, the request should be returned to the author for further action as required. This could be a recommendation for a new date; a request for additional information in further support of the change; or a request for improvement to the implementation and/or back out procedures.

It is the responsibility of the requester to recycle his change through the request and approval process again. In the case of a client generated change request, the Change Control Coordinator will take responsibility for communicating with the client on the status of their particular change request.

8.0 Working Documents

CAT will decide on what action should be taken with each change request. The Team members should have available to them the following documents describing change activities:

- A current change schedule identifying all current and future changes that have been requested.
- Change Requests to be reviewed in those cases where more documentation is required to reasonably evaluate the change.

After discussing the requests, the Team may approve; disapprove; place a change in a pending status indicating that the change itself is approved but not the proposed implementation date or method; or place the change on hold pending future considerations.

9.0 Approval Criteria

The approval decision is based upon five criteria:

State of the production environment: Before determining if a change should be approved, the Team subjectively evaluates the performance and availability of each system in the production environment during the past week. In general, if the production environment has performed well and has been available to the clients, the Team is more likely to approve changes that provide new functionality or changes that might have a high risk of failure. Conversely, if the state of the production environment during the past week has been poor, the Team is more likely to approve only those changes designed to correct problems.

Change level: As part of the approval process, the change level is examined along with the detail information and instructions attached to the Change Request. The attachments should detail the associated risk and impact of the change. Particularly important are the subjective comments provided by the change author indicating the reasons for the assigned change level.

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

nc
7-21-14

Aggregate effect of all proposed changes: The Team is the single place where all of the changes requested for a specific timeframe come together. For example, the Team has the ability to examine several changes, each of which may appear to carry a reasonable risk if taken independently; but when all changes proposed for a particular timeframe are considered as a group, the composite effect may result in too much change activity, hence risk. When the Team reaches this conclusion, their responsibility is to prioritize the various changes, approve the most significant ones, and recommend that the others be re-scheduled.

Resource availability: The Team should be concerned about the availability of people, time, and system resources when considering the scheduling/approval of changes.

Criticality: There are issues that may alter the impact of the change as viewed by the author. For example, the change author may feel that the impact is relatively low because his change affects a small percentage of the client community. However, the Team may judge the criticality to be high because that small percentage includes a client has a critical need.

10.0 The Request Process

Definition of Level Factors

It is the responsibility of the technician or author of a change request to evaluate it against six predetermined categories and assign the Change Level. While the change author normally has a technical perspective with respect to these categories, a business perspective must also be applied when assigning a level.

The six categories consist of:

- Risk
- Impact
- Communication requirements
- Install time
- Documentation requirements
- Education/training needs

Risk considers the probability for success based on the difficulty and complexity of the implementation and back out procedures. The questions that need to be asked are: how certain are you that the change will be implemented successfully the first time; and if the change fails, how sure are you that the fall back procedures will return the system to the same state prior to the change?

Impact analyzes the overall impact to the organization based on machine and people resources. The questions to be asked include: how many people/clients are affected by the change; how much downtime is involved; and how easily can back out be achieved?

Communication requirements takes into account how many clients must be notified of the change and what the logistics are for adequately notifying the affected parties. Can you convey the message with enough time for the recipient to react accordingly? Those responsible for authorizing change must consider the communication requirements.

Install time considers the overall amount of time it takes to prepare the change, implement the change, and recover from a failed change. In other words, if the change takes so long

RC
7-21-2014

Airbus DS Communications Hosting Center

that it cannot be removed with sufficient time to return normal services to clients, it should be leveled high, or be re-worked into a more flexible size.

Documentation assesses the degree to which procedures must be amended to adequately describe what has changed.

Education/training needs considers how significant an impact the change will have on those using or operating the system and what it will take to reasonably expect them to adapt to the new situation.

11.0 Assigning Change Levels

After performing this evaluation, the change author assigns a single designation to his change: Level 3, Level 2, or Level 1.

Level 1 is the most significant change, impacting a large portion of the user community or clients, and/or they are highly disruptive. The back out process is not automatic and requires technical expertise to implement. On site support is required for implementation. Examples of Level 1 changes are: changes to the operating system or major subsystem; application upgrades; changes that are complex to implement. Level 1 changes require a Change Request with at least two (2) weeks advance lead time, and approval from the following: the originating department VP; and Sales Representative; and the Change Approval Team.

Level 2 changes are originated by the Requestor, who may be Hosting Infrastructure or Support personnel. They require coordination among Hosting Infrastructure and Support, and/or the client and have the potential to disrupt a substantial number of users. Examples of Level 2 changes are: new application releases; tools upgrades; configuration changes; hardware changes; restores or any change that Customer Support deems warranting extra control. They include detailed implementation and back out planning. Level 2 changes require a Change Request submitted with sufficient lead-time to allow for planning, scheduling and approval. Approval will come from the Change Approval Team.

Level 3 changes occur daily or on a very frequent basis and are normally non-disruptive or administrative in nature. The impact of failure is either highly unlikely or minimally limited in scope. Examples of Level 3 changes are: new and modified accounts; password resets and DataSync setup. Back out is readily available and reliable. Level 3 changes do not require Change Control paperwork or Change Approval Team approval. They require approval only from the originating department Director.

The risk and impact factors are the two most critical in developing the change level, and the authors of change are advised to weigh these two factors most heavily.

12.0 The Change Request

Once the change level has been established, the change author should communicate the change through the use of a Change Request form. These forms are to be filled out electronically and printed for approval signatures.

13.0 Change Request Lead Times

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

ke
7-21-2015

Airbus DS Communications Hosting Center

Requests for most changes must be submitted with adequate lead time. This lead time will give the coordinator enough time to complete a schedule of proposed changes; distribute the schedule to all group leads and directors and allow the various groups time to communicate with each other regarding coordination or conflict prior to the CAT meeting.

In some instances, changes may be submitted for "tentative" scheduling when they are pending client approval, or when management is considering business impact prior to approval. These changes will be "tentatively" scheduled, presented at the CAT meeting, and considered for any possible conflict with other scheduled changes, and must be clearly identified as 'tentative' by the requestor to avoid having the change rejected due to lack of appropriate approval. The original Change Request with all appropriate signatures must be received before the change will be definitely scheduled for implementation. If the necessary approvals are not received the change will be removed from the activity schedule.

"Late" requests that must be implemented during the current week will be classified as an "Emergency Request" and will require additional approvals; this information will be logged on a weekly and monthly basis and reported on through the Change Management status reports to all Department Vice Presidents.

14.0 Tracking Requests

A ticket is required to be opened with the Help Desk for all implemented or client generated Change Requests. Generation of a Change Request resulting from an Infrastructure initiated service request will be the responsibility of the to which the service request is assigned.

15.0 Disaster Recovery

Disaster Recovery processes are critical to the data center environment, and as such require visibility in the change process. Any change that will alter the current disaster recovery process or documentation must be identified on the change request, and updated documentation provided to the Hosting Center Infrastructure Manager.

The Hosting Center Infrastructure Manager will review all changes being implemented and copy those that have a potential to impact Disaster Recovery. They will perform a follow-up to determine if the change was successful, and if so, request that the update to the Disaster Recovery documentation be made within one week. A secondary follow-up will be performed to ensure that the documentation has, in fact, been updated.

16.0 The Approval Process

Preliminary Approval

Preliminary approval of a Change Request will be completed prior to being submitted to the CAT for final approval and scheduling. It is the change author's responsibility to obtain approval.

The responsible department's director or delegate will complete the primary approval. This will consist of ensuring that testing was completed; modules (if applicable) are ready for production; implementation procedures are provided; the back out processes and procedures are provided; the appropriate date and time have been tentatively scheduled for the change; that the request has been filled out completely; and that the appropriate integrity assurance measures have been taken.

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

He
7-21-2014

Client Acknowledgment

In an effort to ensure that our clients are aware of and prepared for changes to their environments hours of availability, client approval is requested for changes specific to production operating environments. This approval is not always required and will be reviewed on a request-by-request basis. The requester may obtain an email approval or a faxed copy of the request with a client signature, which the requestor will attach to the original request.

Final Approval

The final approval process is conducted at a Change Management Team meeting. The Team will use documented approval criteria when making their decision (see section 9.0, Approval Criteria, of this policy).

17.0 Change Schedule

A preliminary master change schedule will be distributed daily prior to the Change Review meeting to allow each representative time to review the schedule for any conflicts or unidentified impacts. A final master change schedule for the upcoming approved activities will be completed and distributed to all affected parties.

18.0 Emergency Changes

Emergency changes will be classified into one of two categories: "Priority" and "Out of Guidelines." All Emergency changes require approval from: VP of Support and VP of Hosted Services prior to implementation of the change. It is the responsibility of the Change Control Coordinator to escalate and procure all required approvals in an effort to implement the change as expeditiously as possible. Emergency changes do not require review in a Change Approval meeting prior to implementation. All Emergency changes must be fully documented; due to the nature of the request this will often occur after the fact.

Priority: Emergency changes required to fix production problems affecting client critical business functions. These requests must be completed as soon as possible and cannot wait until the next scheduled change window.

Out of Guidelines: Changes which are necessary to support critical client business needs which were not requested with adequate lead time for normal review.

19.0 Review Process

As part of the Change Management process, all changes will be reviewed post-implementation. This process is necessary to ensure that:

- 1) The change procedure was followed
- 2) The change procedure adequately fulfills its objectives
- 3) Implementation and back out procedures were adequate. Problems encountered are discussed for future planning
- 4) Changes are assigned a status of complete, not complete (either partially complete or not at all), failed, backed out, or canceled, as applicable
- 5) The Change Coordinator is responsible for assessing the successful completion of the

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

Re
7-26-2015

Airbus DS Communications Hosting Center

request.

Past changes that were unsuccessful or canceled for any reason will be discussed at the CAT meetings, and a status report will be generated each week distributed to management for review.

A monthly status report, which summarizes the entire month's activity and status, will be generated during the first week of the following month and distributed to management for review. Year-to-date statistics will also be maintained each month and distributed with the monthly status report.

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

Page 38 of 89

KE
7-21-2015

Airbus DS Communications Hosting Center

Customer Support Procedures

1.0 Purpose

The purpose of this document is to define procedures for supporting Hosting Center customers. These support procedures have been defined to ensure a prompt, yet uniform, response to support issues related to Hosting Center infrastructure and customers. These procedures are designed to ensure customers receive a uniform experience with system performance and customer support.

2.0 Scope

This policy is applicable to all Hosting Center, Customer Support, and third-party employees responsible for the support of Hosting Center infrastructure and customers. No employee, contractor, or third party is exempt from these procedures.

3.0 Support Contact Information

Contact Type	Contact Info	Role
Email	Hosting.support@dcusa.com	Email distribution list to contact first-level customer support agents.
Phone Support	615-550-0200	Phone number that contacts first-level customer support agents.
After Hours	615-550-0200	Outside Normal Business Hours calls will be routed to an answering service and the on-call technical analyst is paged. The analyst will return the call within an hour.
Infrastructure Administrator	Unpublished	Infrastructure Administrators are hosting center personnel responsible for configuring the network (servers, security, firewalls, switches) and telephony equipment. IA's provide first-level support to the automated system monitors and second-level support to customer support agents.

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

h
2-1-2015

Airbus DS Communications Hosting Center

Infrastructure Technician	Unpublished	Infrastructure Technicians are responsible for configuring and installing servers and their associated Airbus DS Communications products and applications. IT's provide first-level support to automated system monitors and second-level support to customer support agents.
---------------------------	-------------	---

4.0 First-Level Customer Support

Customer support is composed of technical analysts trained on Airbus DS Communications products to administer and trouble shoot those products and their system configurations. Customers can reach customer support by calling the dedicated ACD phone number or through email.

Calls are routed to a dedicated ACD at 615.550.0200. If a customer calls and receives a recording it means that all Support Desk analysts are at that moment busy assisting other customers. The caller will be transferred to the operator. If the caller is experiencing an emergency they may request that the operator page a support manager to provide assistance.

If the call is not an emergency, they will be put into the support voice mail where they should leave their name, company name and ID, telephone number and a brief description of the reason for the call. Messages are checked frequently and calls are returned in the order in which they are received, but always within four (4) hours. Callers will be given a ticket ID# to use when calling again about the same issue.

Airbus DS Communications' Customer Support desk logs calls in a call tracking system. These calls are then tracked through to resolution as customer support agents, infrastructure administrators, and infrastructure technicians work together to quickly resolve a customer's issue. Customer support agents can escalate calls to IA & IT personnel by assigning the ticket to such personnel in the call tracking system. These second-tier personnel monitor the call tracking system for calls that have been assigned to them. Once a ticket is resolved and closed, the customer support agent who opened the ticket follows up with the customer either by phone or email to acknowledge the issue is resolved.

5.0 Customer Support - Outside Normal Business Hours

If the customer is experiencing an emergency outside Normal Business Hours (defined as 8am – 5pm CST; Monday through Friday, excluding holidays) they should call the support number at 615.550.0200. The call will be routed to a live operator where the customer should leave a clear voice message with their name, company name and ID, telephone number and a brief description of the reason for the call. The on-call technical analyst will be paged and will return the call within an hour.

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

Re
7-26-2015

Airbus DS Communications Hosting Center

Airbus DS Communications Customer Support outside NBH ensures a customer support representative, infrastructure administrator, and infrastructure technician are on-call. Standard business hours, in conjunction with Airbus DS Communications' after-hours program, provide customers 24x7 emergency support. Airbus DS Communications Customer Support After-Hours personnel can be directly contacted by the customer, automated systems monitoring notifications, and other on-call personnel.

6.0 Automated Systems Monitoring and Escalation

Airbus DS Communications' Hosting Center is equipped with state-of-the-art monitoring equipment that monitors the health of all hosted systems, as well as the hosting environment. Hosting Center Infrastructure Administrators define Systems and Environment Monitoring Rules (SEMRs) that recognize system failures and violations of system thresholds (e.g., minimum disk space or maximum allowable CPU usage). System components are then electronically monitored 24x7 for violations of these SEMRs. When a SEMR is violated, the monitor automatically sends an alert to Hosting Center personnel based on skill requirements and escalation rules. Personnel respond promptly to these notifications, on a 24x7 schedule. The system monitors continue to escalate these alerts until responded to. The goal of ubiquitous SEMR monitoring is to detect a failure immediately, or even before there is a failure, to prevent or minimize customer downtime.

7.0 Second-Level Support

Infrastructure Administrators and Infrastructure Technicians provide second-level support to customer support agents. All customer-initiated requests are first routed to the first-level customer support desk. After customer support has logged the issue in the call tracking system and assessed it, they may escalate the issue to the second-level IA and IT personnel when their expertise is required. In order to escalate a ticket for second-level support, the call tracking system ticket must be assigned to the IA or IT personnel.

Second-level support personnel are notified via email when tickets have been assigned to them. They are then required to follow through to investigate or resolve the issue, update the call tracking system ticket with notes accordingly, and notify customer support when the ticket is ready for review and potential closure or reassignment to the appropriate personnel.

8.0 Procedures

There are two primary sources of hosting center support requests: customers (by phone and email) and SEMR monitors. The following describes the procedures followed for each request.

The Customer Support Department will maintain call ownership throughout the entire request process. The Support Desk will address incoming calls as follows.

Step 1	Capture the Request:	A Support Desk analyst will capture all requests by phone, e-mail, or voice mail and verify the right to service based on the customer's name, support contract status and the approved software support list. If the request relates to unsupported software, the customer will be notified. Otherwise, the analyst will continue with Step 2.
--------	----------------------	---

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

Airbus DS Communications Hosting Center

Step 2	Log Request into the Database:	The Support Desk analyst will open a ticket in the call management system. Information included on the ticket will include the customer's name, location, description of problem, severity of problem, and time of request and person reporting the issue.
Step 3	Troubleshoot the Request:	The Support Desk analyst responsible for resolving the call will acknowledge the open ticket and work with the customer to resolve the issue.
Step 4	Escalate to Second Level	The Support Desk Manager will escalate the request to second level support when the first contact is unable to make progress in the resolution of the issue in a timely manner.
Step 5	Log Resolution into the Database:	Support will log the resolutions to requests in the call management database.
Step 6	Verify Customer Satisfaction:	Support will follow up and verify that the customer is satisfied with the resolution.
Step 7	Close the Request or Ticket:	All tickets will be closed after the customer satisfaction has been verified.

System Alert :

- 1) System monitor detects a SEMR violation and pages an on-call infrastructure rep.
- 2) If customer is experiencing downtime, have customer support notify the customer and create a call tracking ticket.
- 3) Infrastructure representative responds to the incident, updating the call tracking system ticket.
- 4) If infrastructure representative can resolve the issue, they notify support for verification and the call tracking system ticket is closed; otherwise the ticket is reassigned.
- 5) Once the issue is resolve, if customer experienced downtime they are updated with a summary of the downtime and cause.

9.0 Roles and Responsibilities

Infrastructure Support is the sole responsibility of the Hosting Center team, Customer Support is the collective responsibilities of the Hosting Center and Customer Support teams. The table below lists organizations with responsibilities related to customer support issues. However, all customer requests must originate with Customer Support who are the first-level support and responsible for coordinating all second-level support.

Airbus DS Communications Hosting Center

Responsibility	Infrastructure Administrator	Infrastructure Technician	Development	Customer Support
First-level customer support				X
Load roster				X
Backup suitcase				X
Create call tracking system tickets ¹				X
Update tickets	X	X		X
Product enhancements or fixes			X	
Firewall configurations	X			
Password changes	X			
Server configurations		X		
Respond to SEMR violation alerts	X	X		
Four-hour response to initial customer contact				X
Notify customer of issue resolution				X

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

he
7-26-2014

Data Privacy Policy

1.0 Purpose

This document defines policy to ensure the privacy and proper handling of corporate and personal data shared with Airbus DS Communications. Airbus DS Communications provides emergency notification services to clients worldwide and acknowledges the responsibility entrusted to us in managing this information and we maintain a commitment to preserve the privacy and integrity of client data.

2.0 Scope

These procedures apply to all Airbus DS Communications employees, contractors, and third-party entities responsible for the installation, configuration, administration, and transportation of hosted customer systems and data. No individual who supports these entities or processes shall be exempt from this policy.

3.0 Policy

All information shared with Airbus DS Communications is subject to Airbus DS Communications' *Information Sensitivity Policy* and *Data Security Policy* and all controls specified therein. This *Data Privacy Policy* governs the hosting and disposal of information, both emergency notification and operational, shared with Airbus DS Communications by its customers. Airbus DS Communications makes every effort to comply with all federal and state laws governing corporate and personal data privacy.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

PC
2-11-14

Data Security Policy

1.0 Purpose

This document defines policy to secure customer data at Airbus DS Communications from first receipt and for as long as that data is managed by Airbus DS Communications, or until such data is destroyed. These measures primarily guide in controlling access to customer data and backup/recovery procedures for this data. Airbus DS Communications maintains a commitment to protect each customer's data.

2.0 Scope

These procedures apply to all Airbus DS Communications employees, contractors, and third-party entities responsible for the installation, configuration, administration, and transportation of hosted customer data. No individual who supports these entities or processes shall be exempt from this policy.

3.0 Policy

This *Data Security Policy* governs the collection, management, and disposal of data, both emergency notification and operational, shared with Airbus DS Communications by its customers.

Data Security, though not restricted to, shall include the following:

- 1) All customer data will be backed up to a removable or offsite media on a daily basis.
- 2) Customer data will be backed up in a manner that permits full recovery to any specified date. These recoveries will include the ability to recover system configuration settings, such as registry settings.
- 3) If data is backed up to removable media, such media will be rotated offsite at least weekly, preferably daily.
- 4) All sensitive customer data is stored on secured hosting center production servers.
- 5) Airbus DS Communications will provide a fax machine in a secured location for transmitting sensitive data.
- 6) Customer data will only be transferred across secure communications media, unless explicitly requested otherwise by the customer.
- 7) A separation of duties shall exist between individuals who authorize data access and personnel who enable data access.
- 8) When an employee or contractor's services are terminated, their system access is terminated as a result of the *Employee/Contractor Termination Policy*.
- 9) When data or hardware that stores data classified as "Airbus DS Communications Hosting Center Confidential" which is defined in the "Information Sensitivity Policy" reaches its EOL, it must be disposed of in a secure manor that prohibits the retrieval of the data by unauthorized parties. EOL is defined as the permanent decommissioning of hardware from a functioning state or the state of customer data after contract termination.
 - a. Hardware that is to be re-purposed that contains confidential data must be sanitized in the following manor.
 - (i) All internal storage devices that are to be reused that contain confidential data must subjected to a process that over writes the entire storage area of the device with a minimum of three passes of random data.

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

pc
7-11-2014

Airbus DS Communications Hosting Center

- (ii) If the storage devices of a hardware system are to be decommissioned, they will be physically destroyed.
- b. Backup media including magnetic tape, optical media and paper will be physically destroyed when it reaches its EOL

Data and systems

In addition to this policy, all data shared with Airbus DS Communications is subject to Airbus DS Communications' *Information Sensitivity Policy* and all controls specified therein.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

Re
7-21-21

Email Security Policy

1.0 Purpose

Email messages sent as a part of notification activations on the production servers or as automated responses to business processes are not routed through the corporate email server and are isolated from the corporate network.

2.0 Scope

This policy covers anti-virus scanning and security of any email sent from a Airbus DS Communications Hosting Center production server email address and applies to all client utilization of these servers.

3.0 Policy

3.1 Prohibited Use

The Airbus DS Communications Hosting Center network email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin.

3.2 Use

The Airbus DS Communications Hosting Center provides email notification as an embedded feature of the services it provides to its clients. Each client has the responsibility to identify that use of email notification from their production servers is consistent with their business needs.

3.3 Monitoring

The Airbus DS Communications Hosting Center may monitor messages without prior notice. The Airbus DS Communications Hosting Center is not obliged to monitor email messages.

3.4 Virus Scanning

The Airbus DS Communications Hosting Center utilizes industry standard anti-virus protection and applies critical updates daily.

3.5 Email Security

Emergency email notifications are secured using embedded user codes used to further validate a user's response.

4.0 Enforcement

Any client that send any emails with inappropriate content as outlined in this policy from any Airbus DS Communications Hosting Center network will be contacted and risk termination of services.

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

he
2-21-20

Employee/Contractor Termination Procedure

1.0 Purpose

This document defines procedures to invoke when an individual's employment or contractor relationship with Airbus DS Communications is terminated.

2.0 Scope

These procedures apply to all Airbus DS Communications employees and contractors, regardless of said individual's physical location. No individual who supports the operations of Airbus DS Communications shall be exempt from this procedure.

3.0 Procedure

The following procedures should be invoked immediately upon completion of an employee or contractor's services to Airbus DS Communications. For an employee, *completion of services* occurs upon completion of Human Resource's exit interview. For a contractor, *completion of services* refers to the last day services are performed for Airbus DS Communications, whether by natural or unnatural termination of said contractor's contract.

- 1) Confirm the individual's building access card, and facility access card is applicable, has been recovered
- 2) If applicable, recover any support pagers in person's possession
- 3) Request Information Technology disable person's corporate LAN account, which also disables their Virtual Private Network (VPN) login
- 4) Request the Information Technology disable person's corporate Exchange email access
- 5) If applicable, disable person's departmental network accounts
- 6) If applicable, disable person's VPN account on the Airbus DS Communications network
- 7) If applicable, contact off-site data facilities to remove access authorization

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

he
-11-20

Encryption Policy

1.0 Purpose

The Purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have proven to work effectively. Additionally, this policy provides direction to ensure that federal regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the United States of America.

2.0 Scope

This policy applies to all Airbus DS Communications employees and customers.

3.0 Policy

Proven, standard algorithms such as 3DES, DES, Blowfish, RSA, RC5, and IDEA should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. For example, Network Associates' Pretty Good Privacy (PGP) uses a combination of IDEA and RSA or Diffie-Hellman, while Secure Socket Layer (SSL) uses RSA encryption. Symmetric cryptosystem key lengths must be at least 128 bits. Asymmetric cryptosystem keys must be of a length that yields equivalent strength. Airbus DS Communications key length requirements will be reviewed annually and upgraded as technology allows. The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by Airbus DS Communications. Be aware that the export of encryption technologies is restricted by the U.S. Government. Residents of countries other than the United States should make themselves aware of the encryption technology laws of the country in which they reside.

4.0 Standards and Key Management

The standard that Airbus DS Communications uses involving encryption and Key Management will be as defined;

- 1) 2048 bits SSL encryption on all web interfaces; SSL signatures shall be used with sha1RSA, 128 bit encryption, Public Key. HTTPS shall be 2048 bit security. Data transferred to and from servers is transferred using Digital Signature, Key Encipherment, and Data Encipherment.
- 2) Data will be encrypted before being stored offsite.
- 3) Copies of public key are kept offline located in a fireproof safe on encrypted media.
- 4) Each VPN Tunnel uses 168 bit 3DES encryption and HMAC MD5 authentication is used to verify integrity.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Definitions

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

Airbus DS Communications Hosting Center

Proprietary Encryption – An algorithm that has not been made public and/or has not withstood public scrutiny. The developer of the algorithm could be a vendor, an individual, or the government.

Symmetric Cryptosystem – A method of encryption in which the same key is used for both encryption and decryption of the data.

Asymmetric Cryptosystem – A method of encryption in which two different keys are used: one for the encryption and one for decrypting the data (e.g., public-key encryption).

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

12
12/12/14

Facility Access Control Policy

This policy as been retired following the relocation of all production servers to outsourced managed data facilities.

Mc
7-11-10

Information Classification & Distribution Policy

1.0 Purpose

The Information Sensitivity Policy is intended to help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of Airbus DS Communications without proper authorization. The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing). All employees should familiarize themselves with the information labeling and handling guidelines that follow this introduction. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that you can take to protect Airbus DS Communications Confidential information (e.g., Airbus DS Communications Confidential information should not be left unattended in conference rooms). *Please Note: The impact of these guidelines on daily activity should be minimal.* Questions about the proper classification of a specific piece of information should be addressed to your manager. Questions about these guidelines should be addressed to Airbus DS Communications.

2.0 Scope

All Airbus DS Communications information is categorized into two main classifications:

- Airbus DS Communications Hosting Center Public
- Airbus DS Communications Hosting Center Confidential

Airbus DS Communications Public information is information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to Airbus DS Communications.

Airbus DS Communications Confidential contains all other information. It is a continuum, in that it is understood that some information is more sensitive than other information, and should be protected in a more secure manner. Included is information that should be protected very closely, such as trade secrets, development programs, customer sensitive information, and other information integral to the success of our company.

A subset of Airbus DS Communications Confidential information is "Airbus DS Communications Third Party Confidential" information. This is confidential information belonging or pertaining to another corporation which has been entrusted to Airbus DS Communications by that company under non-disclosure agreements and other contracts. Examples of this type of information include everything from joint development efforts to vendor lists, customer orders, and supplier information. Information in this category ranges from extremely sensitive to information about the fact that we've connected a supplier / vendor into Airbus DS Communications network to support our operations.

Airbus DS Communications personnel are encouraged to use common sense judgment in securing Airbus DS Communications Confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their manager

3.0 Policy

The Sensitivity Guidelines below provide details on how to protect information at varying sensitivity levels. Use these guidelines as a reference only, as Airbus DS Communications Confidential information in each column may necessitate more or less stringent measures of

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

NC
7-21-14

Airbus DS Communications Hosting Center

protection depending upon the circumstances and the nature of the Airbus DS Communications Confidential information in question.

3.1 Minimal Sensitivity:

General corporate information; some personnel and technical information

Marking guidelines for information in hardcopy or electronic form.

Marking is at the discretion of the owner or custodian of the information. If marking is desired, the words "Airbus DS Communications Confidential" may be written or designated in a conspicuous place on or in the information in question. Other labels that may be used include "Airbus DS Communications Proprietary" or similar labels at the discretion of your individual business unit or department. Even if no marking is present, Airbus DS Communications information is presumed to be "Airbus DS Communications Confidential" unless expressly determined to be Airbus DS Communications Public information by a Airbus DS Communications employee with authority to do so.

Access: Airbus DS Communications employees, contractors, people with a business need to know.

Distribution within Airbus DS Communications: Standard interoffice mail approved electronic mail and electronic file transmission methods.

Distribution outside of Airbus DS Communications internal mail: U.S. mail and other public or private carriers approved electronic mail and electronic file transmission methods.

Electronic distribution: No restrictions except that it is to be sent to only approved recipients.

Storage: Keep from view of unauthorized people; erase whiteboards, do not leave in view on tabletop. Machines should be administered with security in mind. Protect from loss; electronic information should have individual access controls where possible and appropriate.

Disposal/Destruction: Deposit outdated paper information in specially marked disposal bins on Airbus DS Communications premises; electronic data should be expunged/cleared.

Reliably erase or physically destroy media.

Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

3.2 More Sensitive: Business, financial, technical, and most personnel information

Marking guidelines for information in hardcopy or electronic form.

Access: Airbus DS Communications employees and non-employees with signed non-disclosure agreements who have a business need to know.

Distribution within Airbus DS Communications: Standard interoffice mail, approved electronic mail and electronic file transmission methods.

Distribution outside of Airbus DS Communications internal mail: Sent via U.S. mail or approved private carriers.

Electronic distribution: No restrictions to approved recipients within Airbus DS Communications, but should be encrypted or sent via a private link to approved recipients outside of Airbus DS Communications premises.

Storage: Individual access controls are highly recommended for electronic information.

Disposal/Destruction: In specially marked disposal bins on Airbus DS Communications premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

3.3 Most Sensitive: Trade secrets & marketing, operational, personnel (e.g., social security numbers, employee reviews), financial, source code, & technical information integral to the success of our company

Access: Only those individuals (Airbus DS Communications employees and non-employees) designated with approved access and signed non-disclosure agreements.

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

Page 53 of 89

Mc
7-21-14

Airbus DS Communications Hosting Center

Distribution within Airbus DS Communications: Delivered direct - signature required, envelopes stamped confidential, or approved electronic file transmission methods.
Distribution outside of Airbus DS Communications internal mail: Delivered direct; signature required; approved private carriers.

Electronic distribution: No restriction to approved recipients within Airbus DS Communications, but it is highly recommended that all information be strongly encrypted.

Storage: Individual access controls are very highly recommended for electronic information. Physical security is generally used, and information should be stored in a physically secured computer.

Disposal/Destruction: Strongly Encouraged: In specially marked disposal bins on Airbus DS Communications premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Appropriate measures - To minimize risk to Airbus DS Communications from an outside business connection. Airbus DS Communications computer use by competitors and unauthorized personnel must be restricted so that, in the event of an attempt to access Airbus DS Communications corporate information, the amount of information at risk is minimized.

Configuration of Airbus DS Communications -to-other business connections - Connections shall be set up to allow other businesses to see only what they need to see. This involves setting up both applications and network configurations to allow access to only what is necessary.

Delivered Direct; Signature Required - Do not leave in interoffice mail slot; call the mail room for special pick-up of mail.

Approved Electronic File Transmission Methods - Includes supported FTP clients and Web browsers.

Envelopes Stamped Confidential - You are not required to use a special envelope. Put your document(s) into an interoffice envelope, seal it, address it, and stamp it confidential.

Approved Electronic Mail - Includes all mail systems supported by the IT Support Team. These include, but are not necessarily limited to, [insert corporate supported mailers here...]. If you have a business need to use other mailers contact the appropriate support organization.

Approved Encrypted email and files - Techniques include the use of DES and PGP. DES encryption is available via many different public domain packages on all platforms. PGP use within Airbus DS Communications is done via a license. Please contact the appropriate support organization if you require a license.

Company Information System Resources - Company Information System Resources include, but are not limited to, all computers, their data and programs, as well as all paper information and any information at the Internal Use Only level and above.

Expunge - To reliably erase or expunge data on a PC or Mac you must use a separate program to overwrite data, supplied as a part of Norton Utilities. Otherwise, the PC or Mac's normal erasure routine keeps the data intact until overwritten. The same thing happens on UNIX machines, but data is much more difficult to retrieve on UNIX systems.

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

NC
7-26-11

Airbus DS Communications Hosting Center

Individual Access Controls - Individual Access Controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. On PC's, this includes using passwords on screensavers, such as Disklock.

Insecure Internet Links - Insecure Internet Links are all network links that originate from a locale or travel over lines that are not totally under the control of Airbus DS Communications.

Encryption - Secure Airbus DS Communications Sensitive information in accordance with the Acceptable Encryption Policy. International issues regarding encryption are complex. Follow corporate guidelines on export controls on cryptography, and consult your manager and/or corporate legal services for further guidance.

Physical Security - Physical security means either having actual possession of a computer at all times, or locking the computer in an unusable state to an object that is immovable.

Methods of accomplishing this include having a special key to unlock the computer so it can be used, thereby ensuring that the computer cannot be simply rebooted to get around the protection. If it is a laptop or other portable computer, never leave it alone in a conference room, hotel room or on an airplane seat, etc. Make arrangements to lock the device in a hotel safe, or take it with you. In the office, always use a lockdown cable. When leaving the office for the day, secure the laptop and any other sensitive material in a locked drawer or cabinet.

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

Page 55 of 89

Mc
7-21-2015

Network Security Policy

1.0 Purpose

This document defines policy to ensure the security of the hosting center network. The hosting center network is a separate network from Airbus DS Communications' corporate network. These policies intended to preserve the integrity of that network can be categorized by server, firewall, and monitoring policies.

2.0 Scope

These procedures apply to all Airbus DS Communications employees, contractors, and third-party entities responsible for the installation, configuration, and administration of the hosting center network. No individual who supports these entities or processes shall be exempt from this policy.

3.0 Policy

Servers

- Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do.

Firewalls

- The hosting center network will be segregated from the corporate network through firewalls and a separate domain name server.
- Firewalls shall be used to block unauthorized access to Hosting Center infrastructure.
- Firewalls will be configured to report unauthorized access to Airbus DS Communications systems.
- Infrastructure Administrators monitor these logs for opportunities to improve security. These logs are reviewed when prompted by firewall alerts and daily sampling of application logs. Any breach of security or unusual attack on a client's server is reported to that client.
- Firewalls should translate internal addresses to mask the actual name and address of internal machines communicating outside Airbus DS Communications.
- A separation of duties shall exist between personnel who enable system access and those who review audit trails and violation logs.
- Firewalls will be used to implement VPN connections.

Monitoring

- An Intrusion Detection System should be utilized to monitor Airbus DS Communications' network (routers, web servers, mail servers, FTP servers, domain name servers, and firewalls).

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

PC
7-21-20

Password Policy

1.0 Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Airbus DS Communications Hosting Center network. As such, all Airbus DS Communications employees and Hosting Center clients with access to Hosting Center Servers are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.0 Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

3.0 Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Airbus DS Communications Hosting Center facility.

4.0 Policy

4.1 General

All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a quarterly basis.

All production system-level passwords must be part of the InfoSec administered global password management database.

All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months. The recommended change interval is every four months.

User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.

Passwords must not be inserted into email messages or other forms of electronic communication.

Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).

All user-level and system-level passwords must conform to the guidelines described below.

4.2 Guidelines

A. General Password Construction Guidelines

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

me
7-11-10

Airbus DS Communications Hosting Center

Passwords are used for various purposes. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens, (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
 - a) Names of family, pets, friends, co-workers, fantasy characters, etc.
 - b) Computer terms and names, commands, sites, companies, hardware, software.
 - c) The words "<Company Name>", "sanjose", "sanfran" or any derivation.
 - d) Birthdays and other personal information such as addresses and phone numbers.
 - e) Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
 - f) Any of the above spelled backwards.
 - g) Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#\$%^&*()_+|-=<>\{}|'":;<>?,./)
- Are at least eight alphanumeric characters long.
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "Tmb1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

B. Password Protection Standards

Do not use the same password for <Company Name> accounts as for other non-<Company Name> access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various <Company Name> access needs. For example, select one password for the Engineering systems and a separate password for IT systems. Also, select a separate password to be used for an NT account and a UNIX account.

Do not share <Company Name> passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential <Company Name> information.

Here is a list of "don't's":

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't reveal a password to the boss

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

1/c
7-X-26

Airbus DS Communications Hosting Center

- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation

If someone demands a password, refer them to this document or have them call someone in the Information Security Department.

Do not use the "Remember Password" feature of applications (e.g., Eudora, Outlook, Netscape Messenger).

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

Change passwords at least once every six months (except system-level passwords which must be changed quarterly). The recommended change interval is every four months.

If an account or password is suspected to have been compromised, report the incident to Airbus DS Communications Hosting Center staff and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by Airbus DS Communications Hosting Center staff. If a password is guessed or cracked during one of these scans, the user will be required to change it.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Definitions

Application Administration Account Any account that is for the administration of an application (e.g., Oracle database administrator, ISSU administrator).

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

Handwritten signature and date: 2/21/20

Personnel Screening Policy

1.0 Introduction

In order to create a safe and secure workplace and to ensure that Airbus DS Communications employees are qualified to perform the jobs for which the company hires them, the company will conduct pre-employment screening for all regular employees.

2.0 Standard Pre-employment Screening

The Airbus DS Communications Human Resources Department shall check references and verify the educational credentials, employment histories and past performance of a finalist before it extends a final offer of employment.

3.0 Professional License Checks

When an occupation or position requires an employee to have a professional license or certification in order to perform the job, the hiring authority or a designee will verify such license or certification.

4.0 Driving Records

When an occupation or position requires that an employee regularly operates a motor vehicle, the hiring authority or a designee shall work with Human Resources to verify the appropriate license and review the motor vehicle record.

5.0 Criminal History and Identity

When a position is designated as "security sensitive", as are all Hosting Center positions, Human Resources will obtain information on a finalist's criminal history and verification of that individual's identity. This information shall be obtained for individuals not currently employed by Airbus DS Communications, as well as those currently employed by Airbus DS Communications who are seeking "security sensitive" positions. If an individual moves from one "security sensitive" position to another, Human Resources will obtain an updated criminal history.

6.0 Information Collection

A signed authorization from the applicant or finalist is required before criminal background information or pre-employment identity verification may be requested. This information will be collected in coordination with Human Resources. If a prospective employee refuses to provide such authorization, the individual will be ineligible for consideration for such position.

7.0 Information Evaluation

Human Resources shall coordinate all criminal and motor vehicle records screenings, and the reports they produce. Should one of these reports produce information that might prompt an adverse employment action for a current employee, Human Resources will work with the hiring department to evaluate the value of the information against the total past employment record and future employment potential. When considering whether to employ an individual with a criminal history Human Resources will assess the relevance of a criminal conviction to

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

Re
2-21-14

Airbus DS Communications Hosting Center

job duties, the date of the most recent offense, the nature of the offense, and the accuracy of the information the individual provided on the employment application.

Any material misrepresentation or omission on an application document may be grounds for rejection of the application or termination of any subsequent employment with the Company.

8.0 Compliance with the Fair Credit Reporting Act

In some cases, an outside vendor may uncover information that may disqualify an applicant from employment consideration. In such a case, the Company will notify the applicant of the information and provide a minimum of five days for the applicant to refute, explain or correct the information.

9.0 Record Retention

Human Resources will manage and retain criminal pre-employment screening information. Information collected on successful applicants will be stored separately from the official employee files.

10.0 Information Release

Criminal history record information shall be regarded as confidential and only be released consistent with applicable law.

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

Re
7-26-20

Remote Access Policy

1.0 Purpose

The purpose of this policy is to define standards for connecting to Airbus DS Communications Hosting Center network from any host. These standards are designed to minimize the potential exposure to Airbus DS Communications from damages which may result from unauthorized use of Airbus DS Communications Hosting Center resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical Airbus DS Communications internal systems or damage to critical client internal systems.

2.0 Scope

This policy applies to all Airbus DS Communications Hosting Center employees, contractors, clients and agents with a Airbus DS Communications owned, personally-owned or client owned, computer or workstation used to connect to the Airbus DS Communications Hosting Center network.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.

3.0 Policy

3.1 General

- 1) It is the responsibility of Airbus DS Communications employees, contractors, vendors and agents with remote access privileges to Airbus DS Communications Hosting Center network to ensure that their remote access connection is given the same consideration as the user's on-site connection to the Airbus DS Communications Hosting Center network.
- 2) Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of Airbus DS Communications Hosting Center network:
 - a. Encryption Policy
 - b. Virtual Private Network (VPN) Policy
 - c. Wireless Communications Policy
 - d. Acceptable Use Policy
- 3) For additional information regarding Airbus DS Communications Hosting Center network remote access connection options, please contact the Hosting Center Infrastructure Manager.

3.2 Requirements

- 1) Secure remote access must be strictly controlled.
- 2) At no time should any Airbus DS Communications employee provide their login or password to anyone, not even family members.
- 3) Airbus DS Communications employees and contractors with remote access privileges must ensure that their Airbus DS Communications -owned or personal computer or workstation, which is remotely connected to Airbus DS Communications Hosting Center network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
- 4) Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

Re
7-H-245

Airbus DS Communications Hosting Center

homing is not permitted at any time.

- 5) Non-standard hardware configurations must be approved by Hosting Center Infrastructure, and Hosting Center Infrastructure must approve security configurations for access to hardware.
- 6) All hosts that are connected to Airbus DS Communications Hosting Center networks via remote access technologies must use up-to-date anti-virus software, this includes personal computers.
- 7) Personal equipment that is used to connect to Airbus DS Communications Hosting Center networks must meet the requirements of Airbus DS Communications -owned equipment for remote access.
- 8) Remote access to the Airbus DS Communications Hosting Center networks shall be limited to authorized users.
- 9) Authorized users are composed of Airbus DS Communications Infrastructure and Customer Support employees and customers whose business needs require access.
- 10) Remote access users will have their activities logged.
- 11) Remote access activity logs will be monitored with alerts and inspection of random samplings.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Cable Modem - Cable companies such as AT&T Broadband provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps. Cable is currently available only in certain communities.

Dial-in Modem - A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital data of computers into analog signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus the name "modem" for modulator/demodulator.

Dual Homing - Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the Airbus DS Communications Hosting Center network via a local Ethernet connection, and dialing into AOL or other Internet service provider (ISP). Being on a Airbus DS Communications -provided Remote Access home network, and connecting to another network, such as a spouse's remote access.

DSL - Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 6 Mbps downstream (to the user) and slower speeds upstream (to the Internet).

Frame Relay - A method of communication that incrementally can go from the speed of an ISDN to the speed of a T1 line. Frame Relay has a flat-rate billing charge instead of a per time usage. Frame Relay connects via the telephone company's network.

ISDN - There are two flavors of Integrated Services Digital Network or ISDN: BRI and PRI. BRI is used for home office/remote access. BRI has two "Bearer" channels at 64kbit (aggregate 128kb) and 1 D channel for signaling info.

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

re
7-21-20

Airbus DS Communications Hosting Center

Remote Access - Any access to Airbus DS Communications Hosting Center network through a non Airbus DS Communications Hosting Center controlled network, device, or medium.

Split-tunneling - Simultaneous direct access to a non Airbus DS Communications Hosting Center network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into Airbus DS Communications Hosting Center network via a VPN tunnel. VPN Virtual Private Network (VPN) is a method for accessing a remote network via "tunneling" through the Internet.

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

ke
7-21-2015

Security Awareness and Training Policy

1.0 Purpose

The purpose of this policy is to define standards for the Airbus DS Communications Hosting Center Security Training and Awareness Program.

2.0 Scope

The Airbus DS Communications Hosting Center approach is to focus on planning, executing, and assessing training needs while integrating a common training methodology across all affected departments to optimize training effectiveness and efficiency. This policy applies to all Airbus DS Communications Hosting Center Infrastructure and Customer Support staff with access to the Hosting Center network.

3.0 Policy

It is Airbus DS Communications Hosting Center Policy that:

- 1) All Hosting Center Infrastructure and Customer Support staff users accessing Hosting Center Network receive initial Hosting Center awareness training during orientation as a condition of access and thereafter shall complete Hosting Center refresher awareness training as policies are updated, typically each quarter. This shall include security reminders such as e-mail messages, newsletters, posters, etc. to increase security awareness.
- 2) Initial and annual Hosting Center awareness training shall ensure all Hosting Center authorized users and management are familiar with security policies, incident reporting procedures, configuration management, continuity of business operations plan, and disaster recovery.
- 3) Each department will identify, document, track, and report personnel training, certifications, and certification status to the VP of Hosted Services.
- 4) All Hosting Infrastructure and Customer Support personnel shall comply with Hosting Center Security Policies.

4.0 Procedures

- 1) Development and maintenance of a Hosting Center security training and awareness program for all Hosting Infrastructure and Customer Support personnel is required in accordance with this policy.
- 2) Training programs shall be tailored to a user's need-to-know for secure operation or use of the Hosting Center network and related systems.
- 3) The following security areas, at a minimum, shall be addressed during training:
 - a. Workstation configuration and use.
 - b. Management of user identifications and passwords.
 - c. Avoidance and detection of computer viruses.
 - d. Contingency plans, disaster recovery, and procedures for continued operation during emergencies or system failures.
 - e. Detection, response, and reporting of Hosting Center security incidents.
 - f. Overview of Hosting Center security threats (sources and impacts) and vulnerabilities.
 - g. Computer viruses and other malicious code.

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

NC
7-21-2015

Airbus DS Communications Hosting Center

- i. Password management.
 - j. Proper protection, storage, and disposal of SI.
 - k. Proper Internet usage.
 - l. Proper e-mail usage.
 - m. Software use, including awareness of copyright issues and software downloads from the Internet.
 - n. Area and physical security, including challenging strangers and escorting unauthorized personnel.
- 4) Security training and awareness can be accomplished using the following delivery methods:
- a. Airbus DS Communications Hosting Center Policies containing the same subject matter topics.
 - b. Pamphlets.
 - c. Classroom Instruction.
 - d. Placing security awareness training material on a network shared drive with the ability to track successful completion of training.
 - e. Policy Review Meetings
- 5) Hosting Center awareness and training is required for all authorized users before they are granted access to the Hosting Center Network or associated systems. Refresher training shall be conducted annually and when major policy changes occur (e.g., a new policy is implemented).
- 6) A documented process for tracking and reporting training provided to all users, including the name of the person attending, instruction format, dates of attendance, and shall be recorded to ensure compliance with requirements.
-

Security Review and Audit Policy

1.0 Purpose

The purpose of this policy is to establish review and audit requirements for all Airbus DS Communications Hosting Center critical and sensitive systems/applications and to ensure compliance with Hosting Center policies.

2.0 Policy

The Hosting Center Infrastructure Team shall ensure that all critical and sensitive systems/applications and the related infrastructure shall be evaluated as an ongoing process to improve the quality of its operations. This policy shall apply to all facilities.

3.0 Implementation

The Hosting Center review and auditing process can only be performed by the Hosting Center Infrastructure with assessments or checks on a regularly scheduled basis. One level of review typically focuses on a specific system or application and may employ audit functionality. Another level of review is an independent audit which is typically broad enough to include network and Hosting Center Operations activities. The independent audit is typically a formal audit conducted by a contracted vendor.

The implementation of this policy shall be based upon and guided by the use of management-approved security standards and best practices. The following paragraphs specify the information systems auditing policy requirements.

1) System Activity Reviews

In addition to application or system-level audits, information system activity reviews shall be conducted or facilitated by the Hosting Center Infrastructure Team on a periodic basis.

2) Formal Audit Process

An audit process shall be implemented to evaluate Hosting Center systems. These audits or reviews may address physical security, Hosting Center operations security, network security, and Business Continuity and Disaster Recovery. Audit findings shall be documented, properly communicated to the organization, and retained for future reference.

Formal or independent audits may identify problems. The audit findings shall be presented to Hosting Center Senior Management. A written response to the audit findings will be required within 30 days from the report issue date or by the date specified by the auditor, whichever is less. This response shall describe the activities planned by the Hosting Center Infrastructure Team to rectify problems identified in the audit findings report. Hosting Center Senior Management will validate the successful implementation of the corrective action outlined in the response plan.

3) Audit/Review Frequency

All Hosting Center critical applications and systems shall be audited/reviewed after being placed into production. The audit frequency shall be on a periodic basis. Assessment and operational reviews shall be conducted based upon the criticality and risk level of the application.

4) Automated Audit Control Functionality

All systems that process sensitive information or which are considered critical to Hosting Center Operations shall provide for automated audit control functionality if

Airbus DS Communications Hosting Center

technically feasible. The audit control mechanism shall include the following functionality:

- a. Provide the ability to record the start-up and shutdown of each audit;
- b. Capture within each audit record the date and time of the event, type of event, subject identity, objective identity, and the outcome (success or failure) of the event;
- c. Apply a set of rules in monitoring the audited events and, based upon these rules, indicate a potential violation;
- d. Prohibit access to the audit records by all unauthorized users, and to prevent unauthorized deletion or modification of the records;
- e. Create the audit records in a manner suitable for a user to interpret the information;
- f. Provide the ability to perform searches of audit databases on criteria with logical relationships;
- g. Include or exclude auditable events from a set of defined audited events;
- h. Ensure that audit records will be maintained when audit storage is full or an attack has occurred; and
- i. Ensure that those privileged users who have a role as administrator of a network device, operating system, or security software such as a firewall, Intrusion Detection System, etc., will have all events logged.

5) System Audit Logging

The automated audit process shall produce audit logs. All Log data must be classified as sensitive and handled accordingly. These logs must be retrievable through clearly defined procedures and must be maintained for time periods prescribed for audit and recovery purposes. Logging shall occur at the network, operating system and application level if available.

Hosting Center Infrastructure staff must review audit logs to the extent necessary to detect potential security incidents and security breaches.

6) Fault Logging

Faults should be reported and corrective action taken. All hardware or software problems should be logged in order to assist maintenance personnel. If problems persist, a review should also be conducted to ensure that controls have not been bypassed and the system compromised, i.e., unauthorized access to information.

7) Audit Trail Documentation

The audit trail shall include sufficient information to establish what events occurred and who (or what) caused them. Defining the scope and contents of the audit trail information captured will be done carefully to balance security needs with possible performance, privacy, or other costs. In general, an activity event record specification will include: event type, time of event occurrence, User ID associated with the event, program or command used to initiate the event, sensitive data accessed and/or modified, and additional data necessary to investigate and mitigate the event.

8) Access to Audit Logs and Audit Trail Data

Audit logs shall be protected from unauthorized access, modification, or destruction and shall be reviewed periodically for action. Access to logs shall be restricted to those responsible for auditing, those performing assigned maintenance tasks and other approved reviewers.

Access to online audit logs shall be strictly controlled to ensure the integrity of audit trail data against modification. Audit trail records shall be protected by strong access controls to help prevent unauthorized access. Hosting Center Infrastructure staff shall ensure the correct setting of computer clocks for audit log analysis.

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

NC
7-21-2015

Airbus DS Communications Hosting Center

Audit trail software shall also be protected. Controlled access to the event recording mechanism shall be provided.

9) Retention of Audit Logs

Audit logs shall be retained for a specified period (typically one year) regulations. Audit logs shall be backed up and stored off-site, as required, along with the data. In the event of an investigation, audit logs will be kept for an extended period if they are used as evidence in an ongoing investigation.

10) Testing

Hosting Center audits shall evaluate security program compliance with the company's policies and procedures and/or test the effectiveness and the integrity of an information processing system.

Security Testing Policy

1.0 Purpose

To establish the security testing requirements for Airbus DS Communications Hosting Center Infrastructure.

2.0 Policy

Security testing shall be performed on a periodic basis to ensure that information resources are adequately protected. The security testing policy applies to all systems/applications, the network and the physical infrastructure to evaluate the effectiveness of the security measures and controls implemented.

3.0 Roles and Responsibilities

The Airbus DS Communications Hosting Center shall develop standards, enterprise-wide procedures, and guidelines for security testing.

The Hosting Center Infrastructure working with Customer Support shall ensure that security testing is performed on all Hosting Center production systems, the network, and the physical Infrastructure.

Hosting Center Senior Management shall be notified of any vulnerabilities found during testing and shall review and implement controls to minimize the risk associated with these vulnerabilities.

4.0 Implementation

Security testing is performed to protect information from unauthorized modification, loss of use, disclosure, or other threats arising from human or systems-generated activities, malicious or otherwise. Network security testing is performed primarily to identify potential vulnerabilities and remediate them before they affect Hosting Center operations. Physical security testing primarily focuses on the adequacy of internal/perimeter access controls. Policy implementation shall be based upon the use of management-approved security standards and best practices. The following paragraphs specify the Security Testing requirements.

- 1) *Developing a Security Test Strategy.* The Hosting Center Infrastructure Team shall develop a comprehensive test strategy that tests the security of all physical, network and Hosting Center components.
- 2) *General Security Test and Evaluation Process.* The Hosting Center Infrastructure Team shall develop a process that identifies the security test requirements, develops security test plans and procedures, identifies the proper tools for testing, enables testing, evaluates the results, and makes recommendations for improvement.
- 3) *Scheduling Security Tests.* Security testing shall be integrated into the workflow as a normal part of the duties of security administrators to evaluate system security mechanisms and validate that systems are operating properly. The Hosting Center Infrastructure Team responsible for the administration of the Hosting Center network, LAN and systems, shall work with Customer Support to prioritize operational system testing activities according to system criticality, testing costs, and the benefits that testing will provide. Security testing of all sensitive and critical information systems shall be performed at least once per year. Likewise, physical security testing and network security testing shall be performed at least once per year.

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

RC
7-21-2015

Airbus DS Communications Hosting Center

- 4) *Types of Security Tests.* The Hosting Center Infrastructure Team responsible for the administration of the Hosting Center network, LAN and systems, shall work with Customer Support to perform adequate testing to ensure adequate security is being provided in the operating environment. Typically, a combination of several types of security testing techniques is needed to provide a comprehensive assessment of the operational environment. Tests that shall be included in overall security testing strategy for each Hosting Center Facility shall include:
- a. *Network Mapping* – Network mapping involves using a port scanner to identify all active hosts connected to an organization's network, network services operating on those hosts (e.g., file transfer protocol and hypertext transfer protocol), and the specific application running the identified service. The result of the scan is a comprehensive list of all active hosts and services operating in the address space scanned by the port scanning tool.
 - b. *Vulnerability Scanning* – Vulnerability scanners identify not just the hosts and open ports but any associated vulnerabilities automatically instead of relying on human interpretation of the results. Most vulnerability scanners probe for a finite number of problems and attempt to provide information on mitigating discovered vulnerabilities. Vulnerability scanners can be either network scanners or host scanners.
 - c. *Penetration Testing* – Penetration testing is security testing in which evaluators attempt to circumvent the security features of a system based on their understanding of the system design and implementation.
 - d. *Password Cracking* – Password cracking programs can be used to identify weak password usage.
 - e. *File Integrity Checkers* – A file integrity checker computes and stores a checksum for every file to be protected and establishes a database of the checksums. It provides a tool for system administrators to recognize when changes were made to files, particularly unauthorized changes.
 - f. *Anti-Virus and Malicious Code Detection* – Anti-Virus software programs shall be installed to protect both the network and systems in the operating environment.
 - g. *Physical Access Testing* – Physical access testing (both perimeter and internal) shall be performed on a periodic basis (recommend every 3 months). Likewise, physical access testing of the Hosting Center production and network environment shall be performed at similar intervals.
- 5) *Log Reviews.* Various system logs (e.g., firewall logs, Raritan logs, server logs) can be used to identify deviations from security policy. In conjunction with security testing, log review and analysis will provide a more comprehensive evaluation of the operational environment. The Hosting Center Infrastructure Team shall work with Customer Support to perform this evaluation.
- 6) *Recommending Security Enhancements.* Following Security Testing and Evaluation, Hosting Center Senior Management shall consider the recommendations made for improving security and set priorities to keep the risk within an acceptable range.
-

Re
7-21-2015

Security Violation Policy

1.0 Purpose

This document defines the policy of how Airbus DS Communications will react to security violation which occurs within our hosting facilities.

2.0 Scope

These procedures apply to all Airbus DS Communications employees, contractors, and third-party entities responsible for the installation, configuration, and administration of the Airbus DS Communications Hosting Center network. No individual who supports these entities or processes shall be exempt from this policy.

3.0 Policy

Airbus DS Communications monitors its network infrastructure for security breaches using firewall, IDC, and server level tracking.

If a suspected breach is detected by an automated process or infrastructure technician, the Hosting Center Manager is contacted immediately. The Hosting Center Manager will determine whether there has been a breach or there is cause for further investigation and, if so, will then notify the Vice President of Hosted Services.

In the event that a Security breach is confirmed and Airbus DS Communications personnel have reason to believe that customer data may have been compromised, Airbus DS Communications will bring in an independent third party to investigate the validity and extent of the incident. Actions will be taken immediately to isolate and contain any network segment or server that has been compromised. At the earliest opportunity, the Hosting Center Manager or his staff will notify Customer support with details of any systems that have been exposed to the threat and any customers that might have been affected.

At this time resources will be applied to repair any affected system and return the network to a secured state. Once it is confirmed that the security threat has been removed, all customers that may have been affected will be contacted by Customer Support and returned to operational status. Information pertaining to what type of threat their system may have been exposed to as well as help in determining the extent of any data loss will be delivered.

Immediately following a security incident a security review meeting will be called by the Vice President of Hosted Services to review actions taken during the event and discuss potential changes to policies and procedures.

If it is found that a security breach is caused by the direct action of an employee their access rights to protected equipment will be immediately revoked and the matter will be handed over to Airbus DS Communications' HR department.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

re
7-21-2015

Server Security Policy

1.0 Purpose

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by Airbus DS Communications Hosting Center employees. Effective implementation of this policy will minimize unauthorized access to Airbus DS Communications proprietary information and technology.

2.0 Scope

This policy applies to server equipment owned and/or operated by Airbus DS Communications, and to servers registered under any Airbus DS Communications -owned internal network domain. This policy is specifically for equipment on the internal Airbus DS Communications Hosting Center network.

3.0 Policy

3.1 Ownership and Responsibilities

All internal servers deployed at Airbus DS Communications must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment

- Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:

- Server contact(s) and location, and a backup contact
- Hardware and Operating System/Version
- Main functions and applications, if applicable

- Information in the corporate enterprise management system must be kept up-to-date.
- Configuration changes for production servers must follow the appropriate change management procedures.

3.2 General Configuration Guidelines

- Operating System configuration should be in accordance with approved Hosting Center guidelines.
- Services and applications that will not be used must be disabled where practical.
- Access to services should be logged and/or protected through access-control methods such as TCP Wrappers, if possible.
- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with customer requirements.
- Trust relationships between systems are a security risk, and their use should be avoided.
- Do not use a trust relationship when some other method of communication will do.
- Always use standard security principles of least required access to perform a function. Do not use a root account when a non-privileged account will do.
- All system access for hosting center production servers is granted by Infrastructure Management.

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

AC
7-21-2014

Airbus DS Communications Hosting Center

- All system access for corporate servers and workstations is granted by Network Management.
- Only the Infrastructure Administration organization will have access to system administrative tools.
- If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
- Routine access by Hosting Center personnel only access systems using administrative accounts when administrative access is necessary, otherwise, non-administrative accounts are used.
- A separation of duties exists between individuals who authorize system access and personnel who enable system access.
- All unnecessary daemons shall be avoided during the installation process or disabled thereafter.
- All unnecessary services shall be turned off during the installation process or disabled thereafter.
- Only the Infrastructure team is permitted access to disk formatting functions.
- Servers should be physically located in an access-controlled environment.
- Servers are specifically prohibited from operating from uncontrolled cubicle areas.
- The Infrastructure Manager has a super-user account used to support all customer servers.
- Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do.
- When an employee or contractor's services are terminated, their system access is terminated as a result of the Employee/Contractor Termination Policy.

3.3 Monitoring

- All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
 - All security related logs will be kept online for a minimum of 1 week.
 - Daily full tape backups of logs will be retained for at least 1 month.
 - Monthly full backups will be retained for a minimum of 2 years.
- At a minimum, the following information should be logged regarding log in/out activities: user name, user log on date/time, user log out dates/time, and both failed and successful login attempts. Also, file and object access failures, and shutdowns and start ups should be logged.
- Access violations should be logged at the web server and application levels. These logs are reviewed by firewall alerts and daily sampling of application logs.
- A separation of duties shall exist between personnel who enable system access and those who review audit trails and violation logs.
- Security-related events will be reported to Infrastructure Manager, who will review logs and report incidents to Hosting Center management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
 - Port-scan attacks
 - Evidence of unauthorized access to privileged accounts
 - Anomalous occurrences that are not related to specific applications on the host.

3.4 Compliance

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

RC
7-21-2015

Airbus DS Communications Hosting Center

- Audits will be performed on a regular basis by authorized organizations within Airbus DS Communications.
- Audits will be managed by the internal audit. Airbus DS Communications will filter findings not related to a specific operational group and then present the findings to the appropriate support staff for remediation or justification.
- Every effort will be made to prevent audits from causing operational failures or disruptions.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

DMZ - De-militarized Zone - A network segment external to the hosting center production network.

Server - For purposes of this policy, a Server is defined as an internal Airbus DS Communications Hosting Server. Desktop machines and Lab equipment are not relevant to the scope of this policy.

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

Page 75 of 89

NC
7-21-2015

Service Problem & Critical Incident Management Policy

1.0 Preamble

Requests for Airbus DS Communications Hosting Infrastructure assistance and reports of service problems or interruptions are handled routinely by Hosting Infrastructure in conjunction with the Airbus DS Communications Hosting Support staff and associated workflow (see Customer Support Procedures Section). It is appropriate that standards are set for allocation of priorities to these requests and service problems, and that all problems reported to the Hosting Infrastructure staff are managed and escalated effectively. This includes critical incidents affecting a clients significant business functions. The policy covers problem management for all clients and facilities.

2.0 Purpose

This Policy prescribes how service problems and requests for assistance are managed by Airbus DS Communications Hosting Infrastructure. It includes Procedures for allocating priorities to problems, handling routine problems and requests, and for managing critical incidents.

3.0 Scope

The Policy covers all service problems and requests for assistance received by Hosting Center staff for all facilities. This may include service interruptions notified by system monitoring alerts, and Customer Support Staff responding to support requests by clients/users of Hosting Center facilities. All service problems will be recorded into the call tracking software. Some routine requests not affecting any specific clients may not be recorded into the call tracking software, but will be recorded for statistical analysis.

4.0 Policy

All requests for assistance and service problems will be notified to Customer Support and recorded into the call tracking software.

All requests will be prioritized immediately into one of 4 categories:

- Priority 1: Total inability to perform normal operation of any significant business function of the client.
- Priority 2: severely restricts the use of an application, system or piece of equipment affecting significant business functions of the client.
- Priority 3: any problem impacting a group of users where the restriction is not critical to the overall operation of the client.
- Priority 4: any problem impacting only 1 person where the function unable to be performed is not critical to the operation of the client.

A Senior Hosting Infrastructure technician will be on duty during the regular business hours of Hosting Center operations. This staff member will assess and assign Category 1 and 2 priorities depending on the severity of the problem.

Routine requests (Priority 3 and 4) are handled by a set of standard procedures.

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

Mc
7-21-2015

Airbus DS Communications Hosting Center

Problems are escalated if they are not resolved within the following timeframes:

- Priority 1: 30 minutes to Senior Hosting Infrastructure technician
 - Priority 2: 2 hours to Senior Hosting Infrastructure technician
 - Priority 3: 1 working days to Hosting Infrastructure Manager for analysis and action
 - Priority 4: 5 working days to Hosting Infrastructure Manager for analysis and action
- problems escalated to the Hosting Infrastructure Manager will be managed according to the 'Critical Incident Procedure'.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

Page 77 of 89

Mc
7-21-2015

Prioritizing Service Problems Procedure

1.0 Introduction

Provides standards for and processes for categorization of Hosting Center service problems and request for assistance. This is a procedure of the Service Problem and Critical Incident Policy.

2.0 Scope

Covers all problems and requests for assistance notified to Hosting Center Infrastructure and specifies how such problems/requests are prioritized for resolution.

3.0 Procedures

This section defines who allocates priorities and how they are designated. The resolution of service problems should be managed in priority order. Customer Support normally allocates priorities as requests/problems are received. Hosting Center Infrastructure staff will be responsible for monitoring system alerts and reporting problems to Customer Support for logging service problems into the call tracking software where specific clients are effected. Where a Priority 1 or 2 problem is suspected, Customer Support or other Hosting Infrastructure staff member **MUST** notify the Senior Hosting Infrastructure technician immediately.

Priority 1

Priority 1 is defined as the **total inability** to perform the normal operation of any significant business function of the client. This could be caused by system unavailability, major hardware failure, network failure or software problems. The result is that the affected function cannot operate normally, and the problem causes a major impact to client services. Services affected by a Priority 1 problem are classified as important and must be fixed urgently.

1) Affects:

The client service as a whole

Significant client business function originating from a complete network outage at a either facility.

2) Critical Services: includes but not limited to -

Client application	Web Servers	Automatic Imports
Web Interfaces	Network Services	DataSync
MS SQL	Phone -PABX	

3) Examples:

- All users or administrators unable to login.
- Failure in the network, impacting either facility.
- Client Interface unavailable.
- Loss of e-mail or voice notifications.
- Server is unavailable for DataSync operations.

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

nc
7-21-201

Priority 2

Priority 2 problems severely restrict the use of an application, system, or piece of equipment affecting significant business functions of the client. This can result in a serious re-scheduling of business resources, and if it continues can result in severe degradation of service - Facility wide or individual client servers.

In the absence of a Priority 1 problem, a Priority 2 problem may assume the place of a Priority 1 problem.

1) Affects:

Hosted Services over a number of clients.

2) Examples:

Activation Reports not sent automatically.

Automatic data import files rejected.

Priority 3

A Priority 3 problem is any problem impacting a group of users where the restriction is not critical to the overall operation of the client service.

A Priority 3 problem does not require an immediate fix. This would normally indicate that there is no significant loss of service or client operations. A Priority 3 problem can also be a request considered urgent to the customer.

1) Affects:

A group of users or critical contact member.

2) Examples:

Individual telephone lines are unavailable for notifications.

Additional paging scripts need to be introduced to the system.

Priority 4

A Priority 4 problem is any problem only impacting one person where the function unable to be performed is not critical to the operation of the client.

A Priority 4 problem may take an extended period before being resolved, but should be attended to as soon as possible and within agreed timeframe with client.

1) Affects:

An individual user.

2) Examples:

Information request.

Re
7-21-20

Airbus DS Communications Hosting Center

Application setup issues.

Establishing the Correct Priority

Customer Support normally receives and enters problems/request into the call tracking software. The Senior Hosting Center technician MUST be notified when a Priority 1 or 2 problem is suspected. The Senior Hosting Center technician must assess the extent of the services affected (number of clients/users, what services) and allocate Priorities as soon as possible.

A Hosting Center customer may indicate that their problem warrants a higher Priority than that assigned by the Hosting Infrastructure Staff according to the above definitions. The Hosting Center Infrastructure staff uses the following guidelines to assist in determining the true Priority of a problem:

- How many users are affected, and what is the impact to the business?
 - Can the problem wait till the next working day?
 - Is there an alternative way to carry out the work (i.e. manual process)?
 - What type of work is being affected, i.e. production or testing?
 - Is the production limitation holding up the clients business need, or can they continue working without this service?
 - How urgent or important is this activation?
 - Will a customer contact be available assist in problem resolution?
 - Will access to replacement hardware/equipment be available if required?
-

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

Re
7-21-2015

Critical Incident Management Procedure

1.0 Purpose

These instructions provide a standard procedure for managing Priority 1 and 2 service problems for the IT services provided by ITS.

This procedure is linked to the Service Problem and Critical Incident Policy.

2.0 Scope

Covers Priority 1 and Priority 2 problems where a failure in an Hosted Center system has resulted in the total inability or severe restriction to perform the normal operation of a significant business function of the client.

3.0 Procedures

High priority problems may be identified in a number of ways:

- Calls coming into the Customer Support Desk;
- Alerts from systems monitoring tools such as Mercury™ Sitescope and HP's Insight Manager; and
- Technical support staff identifying a problem.

The Senior Hosting Infrastructure technician identifies Priority 1 and 2 problems referred from Customer Support and ensures that the correct follow up/escalation procedure is carried out. All Priority 1 and 2 problems must be referred to the Senior Hosting Infrastructure technician immediately if a 'quick fix' is not available so that a central point of coordination occurs. The Senior Hosting Infrastructure technician is also responsible for keeping stakeholders informed of the problem progress.

Where technical staff identifies the existence of a Priority 1 or 2 problem, they should assess what to do from the following:

- If the problem can be fixed quickly (i.e. less than 10 minutes), technical staff may proceed to fix the problem without sending downtime notice.
- If the problem requires more time to resolve, Customer Support should be notified as soon as possible (5-10 minutes after problem realised), and a downtime message issued as soon as possible.

It is important that technical support staff notify Customer Support as soon as possible and do not spend 5-10 minutes (which can quickly lead into much longer) working on diagnosis and resolution before they notify anyone. If it is a real quick fix scenario, or immediate action is required to prevent damage, then work should be undertaken straight away.

The Senior Problem Manager is responsible for:

Receiving/detecting high priority problems

Customer Support receives/detects potentially Priority 1 and 2 problems from customers.

Performing initial assessment

Carries out initial assessment to determine extent of service/s affected and decides whether the problem is Priority 1 or 2. Liaises with the appropriate area to perform technical checks to determine where the problem lies and which Infrastructure Section the problem should belong to and to allocate the problem to them.

Re
- 11-2015

Airbus DS Communications Hosting Center

These initial technical checks should take no more than 10 minutes and feedback must be provided to the Senior Problem Manager so that he/she may continue to co-ordinate the problem. The Senior Problem Manager must take initiative to ensure feedback is provided if none has been received within the allotted time.

Allocating the problem to a Support Section

Ensure that correct Support Section has been notified and is ready to work or is working on the problem.

Notify the Hosting Infrastructure Manager

As soon as possible after extent of service difficulty is known; contact the Critical Incident Manager to provide initial details of the problem, extent of services affected and resolution efforts.

Priority 1 - escalate to the Critical Incident Manager under the Critical Incident Manager Procedure at 30 minutes after initial detection.

Priority 2 - escalate to the Critical Incident Manager under the Critical Incident Manager Procedure at 2 hours after initial detection.

If the problem does not look resolvable within the above timeframes, escalate to Hosting Infrastructure Manager immediately. The Senior Hosting Center technician is required to use discretion and decide if it is necessary to escalate the problem to the Hosting Infrastructure Manager before the above timeframes.

Liaising with Hosting Infrastructure Manager

Continue to liaise with the Hosting Infrastructure Manager until the problem is resolved. Further co-ordinate and organize information updates to stakeholders (eg, Customer Support and Hosting Management) until resolution of problem is reached.

4.0 Role of Hosting Infrastructure Manager

When a Priority 1 or 2 problem occurs, the Critical Incident Manager is responsible for:

Client communications

Liaise with Customer Support Manager to ensure all affected clients are aware of the problem status and Customer Support has communicated the relevant information to them in a timely manner. Ensure that Customer Support staff are continually updated via Senior Hosting Center technician.

Senior Management communications

Ensure applicable senior Managers have been made aware of the problem. This would include the Executive VP, Hosted Services VP, and Support VP.

Correct resources have been allocated to the problem

Check that correct resources have been allocated to resolving the problem. For example, do we have the correct team working on the problem and are the team members sufficiently experienced to cope with such a problem?

Remove any obstacles hindering the resources from concentrating on the problem. Examples of this would be too many people requesting problem updates, access to certain skill groups, etc. Whatever is needed, it is the Hosting Infrastructure Manager's job to ensure they receive it.

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

12
7-11-2015

Initial Contingency Actions

Meet with Support VP and/or support team and determine what immediate contingency actions are possible.

Vendor support

Ascertain whether consideration has been given to calling upon the vendors.

Ongoing problem resolution

If the problem is not resolved within 3 hours, Hosting Infrastructure Manager should call meeting to:

- get a full briefing from support staff working on problem;
- undertake analysis of effects and ongoing risks;
- review the approach to problem resolution;
- determine an alternative courses of actions (if possible);
- develop contingency plans;
- ensure appropriate resources are allocated (including vendor support);
- confirm client communications with Customer Support; and
- confirm the brief to Hosting Center senior management.

Depending on the type of problem, the Hosting Infrastructure Manager should determine frequency of team meetings and ensure meetings are held. It is recommended that Critical Incident meetings are held every 3 hours. Given a protracted outage, a situational assessment should be made near close of business each day (i.e. 4.00 pm).

Service restoration and review

Once the problem is resolved, the CIM must:

- notify Customer Support;
 - notify Hosting Center Senior Management;
 - conduct formal review of problem/problem resolution process to document lessons learnt and compile an outstanding issues list for ongoing work.
 - log critical incident in central repository.
-

Software Maintenance Policy

1.0 Purpose

This document defines policy for performing routine maintenance of hosting center systems. Due to the need for O/S updates, application upgrades, Airbus DS Communications product hot fixes, and the day-to-day growth of system files all systems require a maintenance plan. These maintenance activities should be scheduled to minimize customer interference, downtime, and emergency system restore time.

2.0 Scope

These procedures apply to all hosting center systems hosting customer products and implemented in conjunction with the Airbus DS Communications' *Change Management Policy* and *Change Management Procedures*. No individual who supports the operations of Airbus DS Communications shall be exempt from this policy.

3.0 Procedure

Maintenance routines should be implemented incrementally over time to minimize risks. Once the maintenance routine is being implemented manually then it should be automated and scheduled to run during a regularly scheduled window each week. The following tasks should be performed on all customer servers at least weekly.

Until maintenance is automated, a maintenance schedule will be published to notify customer of their maintenance window and maximum amount of expected downtime.

Routine Maintenance:

- Windows updates – With W2K servers, these updates can be scheduled for automatic updates. However, some updates cannot be applied on an automated schedule and must be manually applied.
- Application upgrades – applications, such as Norton Anti-Virus, get updates published regularly. There should be a coordinated plan for applying these updates.
- Defrag – hard disk data becomes fragmented with use and should be defragmented at least monthly.
- Log file maintenance Review – Databases, applications and operating systems produce log and archive files that, left unattended, can grow to excess sizes. These files may need to be reviewed for possible errors and then purged and or archived if needed.
 - 1) Event logs are viewed manually each maintenance window or more frequently if deemed necessary. Technicians look for warning and error messages that could suggest problems in the Airbus DS Communications application, Microsoft updates or hardware of a hosted system.
 - 2) Transaction Logs on systems with Microsoft SQL server are monitored to insure that the logs are truncated and backed up after a full database backup is accomplished.
- Empty Window's recycle bin.
- Reboot server
- Logout of server
- Verify the system is live again.

Non-Routine Maintenance:

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

RC
7-21-2015

Airbus DS Communications Hosting Center

- Hot Fixes – periodically Airbus DS Communications releases hot fixes for its products. There should be a coordinated plan for applying these updates.

All maintenance activities shall be preceded by nightly backups. Furthermore, it may be necessary at times to recover from a faulty upgrade, especially automated vendor upgrades. For this reason, utilization of a ghosting or recovery manager tool is recommended for quick recovery. Such solutions must be capable of recovering system configuration settings such as registry changes.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

Page 85 of 89

11c
7-21-2015

System Monitoring Policy

1.0 Purpose

The purpose of the Monitoring Policy is to ensure that Proactive infrastructure health and performance monitoring controls are in place. Airbus DS Communications uses system and software monitors to ensure the health and performance of all hosted customer systems. Monitors provide trend information that can identify problems long before they impact the function of our hosted systems. Monitoring our systems also ensures that we meet our system uptime requirements. In the event of a monitor reporting data out of limits for normal activity, email and pager notifications are sent to hosting center staff. These notifications are resent until resolution of the problem.

All customer systems in the hosting center are observed with the following monitoring package.

- **CPU Utilization Monitor**

Report the percentage of CPU currently in use to ensure that you know if the CPU is being overloaded.

- **Disk Space Monitor**

Report the percentage of disk space currently in use so that you can act before you run out of disk space.

- **Memory Monitor**

Measure virtual memory usage and receive proactive notification of problems.

- **Network Monitor**

Track network statistics for your server. Information provided by the network monitor can help you track down performance problems related to network interfaces on your servers.

- **Service Monitor**

Verify that specified processes are running, including Web, Mail, FTP, News, Gopher, Telnet, and DNS. (as required)

- **URL Monitor**

Verify availability and access time for specified URLs to ensure Web pages are available within an acceptable time frame. On Windows NT, SiteScope takes advantage of the platform's integrated support to monitor secure HTTPS URLs in addition to HTTP URLs. (as required)

- **FTP Monitor**

Verify that a file can be retrieved from a file transfer protocol (FTP) server. (as required)

- **Ping Monitor**

Verify that specified hosts are available via the network to ensure continuous availability of critical connections.

- **Operator Monitoring**

During the maintenance period every week, our hosting center staff personally checks each system for proper function. Some of their tasks include:

1. Checking Application logs.

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

RC
7-26-2015

Airbus DS Communications Hosting Center

2. Checking Windows event logs.
3. Test application functionality.
4. Check and apply required OS patches.

There are some cases when increase monitoring is required to help with problem resolution or system sizing. In these cases Airbus DS Communications could choose to employ additional monitors. The following is an example of some of the additional monitors available.

- **Composite Monitor**

Monitor the status readings of multiple monitors or multiple groups of monitors. Create alerts based upon more than one status reading.

- **Database Monitor**

Verify database queries.

- **Directory Monitor**

Monitors file count and size within a directory.

- **File Monitor**

Monitor file system parameters such as the size, age, and content of a file, and receive notification of any changes.

- **Log File Monitor**

Generate warnings and errors based upon data in an application's log file. For example, many applications write error messages to a log file. This monitor can scan those log files, looking for error messages and generating alerts when it finds them.

- **NT Event Log Monitor**

Watch one of the Windows NT Event Logs (System, Application, or Security) and trigger alerts when entries are added.

- **NT Performance Counter Monitor**

Retrieve the value of any Windows NT Performance Counter and send alert if this value is out of a specified range.

- **URL Content Monitor**

Retrieve a selected URL, checking for multiple strings of text within the page.

- **URL Sequence Monitor**

Verify a session that includes multiple pages. An example of this would be entering an account name via a Web form and checking an account status for the page that is returned.

- **Web Server Monitor**

Report data recorded by the Web server log such as hits, bytes, errors, hits per minutes and bytes per minute.

- **Web Service Monitor**

Send SOAP requests to a Web Service enabled application to verify availability.

- **Link Check Monitor**

Monitor all internal and external Web site links for link integrity.

- **DNS Monitor**

Airbus DS Communications Confidential

Copyright © 2014 Airbus DS Communications, Inc. All rights reserved.

AC
7-21-2015

Airbus DS Communications Hosting Center

Verify that the Domain Name Server (DNS) is accepting requests. Verify that the address for a specific domain name can be found.

- **Mail Monitor**

Verify that the mail server is accepting requests, and that messages can be sent and retrieved.

- **Port Monitor**

Determine whether a service on a port can be connected to.

Virtual Private Network (VPN) Policy

1.0 Purpose

The purpose of this policy is to provide guidelines for Remote Access IPsec or SSL Based Virtual Private Network (VPN) connections to the Airbus DS Communications Hosting Center network.

2.0 Scope

This policy applies to all Airbus DS Communications Hosting Center employees, contractors, consultants, temporaries, customers and other workers including all personnel affiliated with third parties utilizing VPN to access the Airbus DS Communications Hosting Center network.

3.0 Policy

Approved Airbus DS Communications employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPN, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees. Additionally,

1. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to Airbus DS Communications Hosting Center networks.
2. VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong pass phrase.
3. When actively connected to the Hosting Center network, VPN will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.
4. Dual (split) tunneling is NOT permitted; only one network connection is allowed.
5. VPN gateways will be set up and managed by Airbus DS Communications infrastructure operational groups.
6. All computers connected to Airbus DS Communications Hosting Center networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard (provide URL to this software); this includes personal computers.
7. VPN users will be automatically disconnected from Airbus DS Communications Hosting Center's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
8. The VPN concentrator is limited to an absolute connection time of 24 hours with the exception of site-to-site VPN connections between facilities.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.
