

# NASA

National Aeronautics and Space Administration

Office of Inspector General

Office of Audits

# NASA'S MANAGEMENT OF THE NEAR EARTH NETWORK

March 17, 2016

Report No. IG-16-014





## **Office of Inspector General**

To report, fraud, waste, abuse, or mismanagement, contact the NASA OIG Hotline at 800-424-9183 or 800-535-8134 (TDD) or visit <https://oig.nasa.gov/hotline.html>. You can also write to NASA Inspector General, P.O. Box 23089, L'Enfant Plaza Station, Washington, D.C. 20026. The identity of each writer and caller can be kept confidential, upon request, to the extent permitted by law.

To suggest ideas for or to request future audits contact the Assistant Inspector General for Audits at <https://oig.nasa.gov/aboutAll.html>.



# RESULTS IN BRIEF

## NASA's Management of the Near Earth Network

NASA Office of Inspector General  
Office of Audits

March 17, 2016

IG-16-014 (A-15-007-00)

### WHY WE PERFORMED THIS AUDIT

NASA's Near Earth Network, part of the Agency's Space Communications and Navigation Program, provides tracking, telemetry, and command services to approximately 40 NASA science missions operating in low Earth orbit and will be used to support the Space Launch System (SLS) and Orion Multi-Purpose Crew Vehicle (Orion) scheduled to launch before the end of the decade. The Network also supports other Federal agencies, including launch and contingency support for National Oceanic and Atmospheric Administration's satellites that assist with weather forecasting for the United States. To provide these services, the Near Earth Network uses NASA-owned antennas and transmitters, as well as equipment owned by other U.S. or foreign government agencies or commercial providers.

Using non-Government entities to transmit Network data presents significant security challenges. Moreover, NASA's Network assets are located in extreme environments such as Alaska and Antarctica, making maintenance on the aging structures more difficult. Constrained budgets have also led the Agency to defer some maintenance activities, which, on at least one occasion, has contributed to the unexpected failure of Network equipment.

We performed this audit to assess whether NASA is properly ensuring the information technology (IT) and physical security of the Network and managing Network capabilities to meet current and future requirements within cost, schedule, and performance goals. We reviewed appropriate policies, procedures, regulations, and conducted interviews with personnel from NASA's Office of Protective Services, as well as personnel at the Alaska Satellite Facility and Universal Space Network's North Pole Ground Station Facility. In addition, we reviewed the implementation of management, operational, and technical controls on the Network assets and focused our efforts on key areas of risk management, security awareness, and continuous monitoring.

### WHAT WE FOUND

By deviating from elements of Federal and Agency cyber and physical security risk management policies, NASA, Goddard Space Flight Center (Goddard), and the Near Earth Network Project Office increased the Network's susceptibility to compromise. Specifically, NASA assigned a security categorization rating of "Moderate" to the Network's IT systems and did not include the Network in its Critical Infrastructure Protection Program. We believe this categorization was based on flawed justifications and the Network's exclusion from the Protection Program resulted from a lack of coordination between Network stakeholders. Given the importance of the Network to the success of NASA Earth science missions, the launch and contingency support it provides for Federal partners, and its importance in supporting human space flight in the future, we believe a higher categorization and inclusion in the Protection Program is warranted.

We also found that information system connections between the Network and the external entities that support its operations are not managed in accordance with Federal and NASA policy. As a result, the Agency does not have sufficient visibility into the security posture of these external systems and cannot ensure the owners are able to adequately respond to or report security events. In addition, IT security controls, such as software that identifies

malicious code, are not in place or functioning as intended. Moreover, due to insufficient coordination between the Network, Goddard, and NASA Office of Protective Services physical security controls have not been implemented on NASA-owned and supporting contractor facilities in accordance with Agency or Federal standards.

Finally, Network components are at risk of unexpected failure due to their age and lack of proactive maintenance. Although the Network is performing preventative maintenance on NASA-owned assets, it has not been performing or tracking depot-level maintenance on this equipment. This failure to proactively inspect and replace cables and mechanical systems that are reaching their failure point has already resulted in one unexpected breakdown and could require the Network to purchase more costly commercial services in the future.

## WHAT WE RECOMMENDED

---

We made 14 recommendations to NASA, including that the Agency include the Network in its Critical Infrastructure Program, recategorize the Network as a “High” system and implement the corresponding security controls, review all external system connections to ensure they are in accordance with NASA policy, and perform and track deferred depot-level maintenance.

NASA management concurred or partially concurred with our recommendations and described planned corrective actions. With the exception of Recommendation 2, we consider management’s comments responsive and therefore have resolved and will close the recommendations upon completion and verification of the proposed corrective actions. With regard to Recommendation 2, management agreed to recategorize the portion of the Network that supports the SLS and Orion as a “High” system, but intends to retain the “Moderate” rating for the rest of the Network because it is not critical to the operation of any NASA spacecraft or spacecraft program. As discussed in our report, we do not believe the Network operates simply as a “pass through” for communications. Rather, Network components must store (albeit temporarily) and process data and commands prior to transmission to the spacecraft. Given the importance of the Network to the success of NASA Earth science missions and the launch and contingency support it provides other Federal agencies, we continue to believe the entire Network should be categorized as “High.” Accordingly, Recommendation 2 is unresolved.

**For more information on the NASA Office of Inspector General and to view this and other reports visit <http://oig.nasa.gov/>.**

# TABLE OF CONTENTS

<b>Introduction</b> .....	1
Background .....	1
Organizational Reporting Structure of the Near Earth Network .....	5
Information Technology and Physical Security Management of Network Assets.....	6
<b>Network Security Management Not Compliant with Regulations and Lacks Necessary Elements for Effective Security</b> .....	9
Network Not Protected as Mission-Essential Infrastructure .....	9
NASA Lacks Visibility of the Security Posture of the Network’s External Information System Connections.....	12
Inadequate Continuous Monitoring of the Network.....	13
Physical Security Controls Not in Compliance with Federal and NASA Policies .....	17
<b>Inadequate Maintenance of Ground Stations Could Increase Costs</b> .....	20
Depot-Level Maintenance Not Performed or Tracked as Deferred Maintenance .....	20
Depot-Level Maintenance is Essential to Reliable Ground Station Operations .....	21
<b>Conclusion</b> .....	23
<b>Recommendations, Management’s Response, and Our Evaluation</b> .....	24
<b>Appendix A: Scope and Methodology</b> .....	27
<b>Appendix B: NIST Risk Management Framework and Associated Federal and NASA Guidance</b> .....	30
<b>Appendix C: Management’s Comments</b> .....	31
<b>Appendix D: Report Distribution</b> .....	38

# Acronyms

---

CIO	Chief Information Officer
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
FY	Fiscal Year
GAO	Government Accountability Office
IT	Information Technology
ITCD	Information Technology and Communications Directorate
NIST	National Institute of Standards and Technology
NOAA	National Oceanic and Atmospheric Administration
NPD	NASA Policy Directive
NPR	NASA Procedural Requirements
OCIO	Office of Chief Information Officer
OIG	Office of Inspector General
OPS	Office of Protective Services
PIV	Personal Identity Verification
SCaN	Space Communications and Navigation
SLS	Space Launch System
SMAP	Soil Moisture Active Passive
SOC	Security Operations Center
SP	Special Publication

# INTRODUCTION

The Near Earth Network, part of NASA's Space Communications and Navigation (SCaN) Program, provides tracking, telemetry, and command services to approximately 40 Agency science missions operating in low Earth orbit, including the recently launched Soil Moisture Active Passive (SMAP) mission and the Aura mission, which is still operating more than 10 years after its 2004 launch.<sup>1</sup> The Network also provides launch and contingency support for the National Oceanic and Atmospheric Administration's (NOAA) National Environmental Satellite, Data, and Information Service Program satellites, which provide weather forecasting for the United States. To provide these services, the Near Earth Network uses NASA-owned antennas and transmitters located in Alaska, New Mexico, Virginia, and Antarctica, as well as equipment in other parts of the world owned by other U.S. or foreign government agencies or commercial entities. Although as of fiscal year (FY) 2014, the Network relied on commercial entities to deliver about half of the services it provides, beginning in FY 2015 the Network will see a significant increase in services through NASA-owned ground stations.

Using non-U.S. Government entities to transmit Agency data presents significant security challenges. Moreover, NASA's own Network assets are located in extreme environments and aging, making maintenance more difficult. Constrained budgets have also led the Agency to defer some maintenance activities, which, on at least one occasion, has contributed to the unexpected failure of Network equipment.

The overall objective of this audit was to assess whether NASA is properly ensuring the information technology and physical security of the Near Earth Network and adjusting Network capabilities to meet current and future requirements within cost, schedule, and performance goals. This is the third in a series of audits by the Office of Inspector General (OIG) examining the various Networks managed by the SCaN Program.<sup>2</sup> See Appendix A for details of the audit's scope and methodology.

## Background

---

The Near Earth Network traces its heritage to the 1960s when NASA implemented its first ground-based communications network to support a growing demand for satellite tracking as well as the Mercury, Gemini, and Apollo human space flight programs. As the need for space communications continued to increase, NASA found its original network insufficient. Accordingly, in the 1990s NASA dedicated a set of ground-based stations to provide communications support for science missions in low Earth orbit, which became the Near Earth Network. The Agency also developed a separate system, the Space Network, to support the communication needs of Space Shuttle missions and the International Space Station.

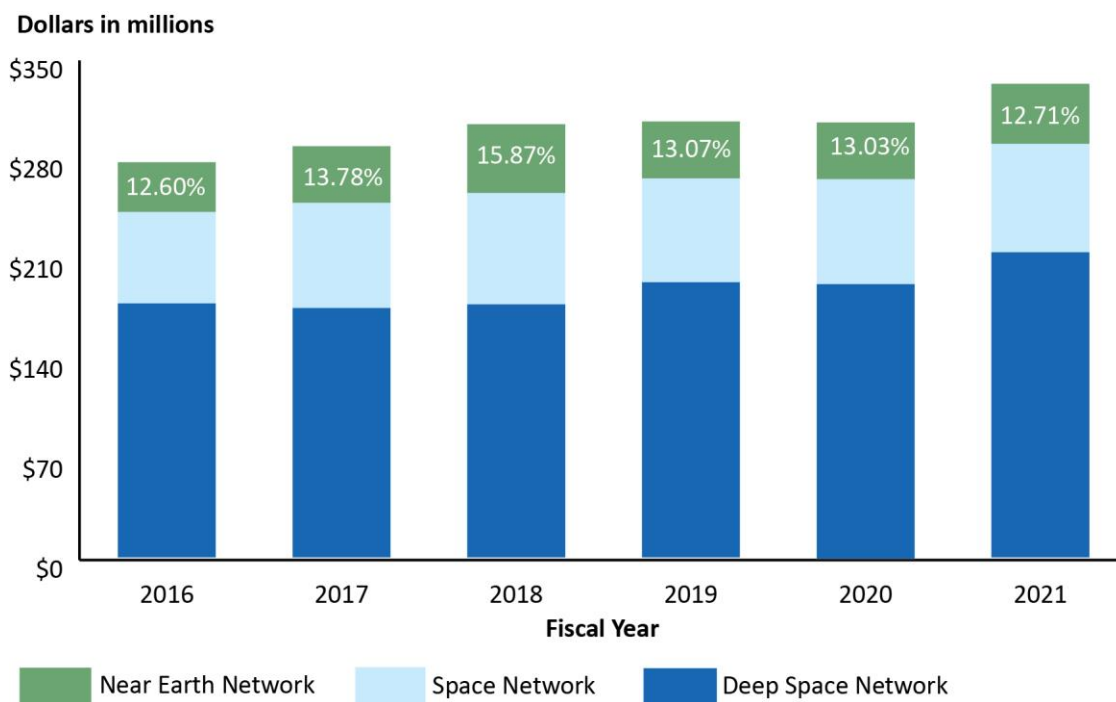
---

<sup>1</sup> Launched in January 2015, SMAP was designed to help scientists understand the links between Earth's water, energy, and carbon cycles and to enhance the ability to monitor and predict natural hazards like floods and droughts. Aura studies the chemistry of the Earth's atmosphere by taking measurements that enable scientist to investigate questions about ozone trends and air quality changes and their linkage to climate change.

<sup>2</sup> NASA OIG, "Audit of NASA's Management of the Deep Space Network" (IG-15-013, March 26, 2015); "Audit of the Space Network's Physical and Information Technology Security Risks" (IG-14-026, July 22, 2014); and "Space Communications and Navigation: NASA's Management of the Space Network" (IG-14-018, April 29, 2014).

The SCaN Program manages the Near Earth Network, the Space Network, and a third space communications system – the Deep Space Network – which supports missions operating beyond geosynchronous orbit.<sup>3</sup> Of the three networks, the Near Earth Network’s budget is the smallest, accounting for approximately 13 percent (or an annual average of about \$40 million) of the Agency’s operating budgets for the Networks (see Figure 1).

**Figure 1: Projected FY 2016–2021 Operating Budgets for NASA’s Space Communication Networks**



Source: NASA OIG analysis of SCaN Program data.




Note: Percentages reflect the Near Earth Network’s portion of the Networks’ operating budgets.

The Near Earth Network provides tracking, communications, and data system services to support pre-flight, launch, orbital, landing, and post-flight activities. The Network’s customers include NASA’s Science, Human Exploration and Operations, and Space Technology Mission Directorates, as well as other Government agencies, international civilian space agencies, and commercial entities. Most of the missions the Network supported in 2015 were investigating various aspects of the Earth’s atmosphere, hydrology, geography, geology, and ecology. Figure 2 provides a summary of three missions supported by the Network.

<sup>3</sup> A geosynchronous orbit is an orbit in which a satellite is always in the same position in respect to the rotating Earth. Satellites in this orbit sit above 35,000 kilometers.



**Figure 2: Sample of Missions Supported By Near Earth Network**

	<b>Science</b>	<b>Mission Characteristics</b>
<b>AQUA</b>	 <p>Carries six state-of-the-art instruments to observe the Earth's ocean, atmosphere, land, ice and snow covers, and vegetation, providing high measurement accuracy, spatial detail, and temporal frequency.</p>	<p><b>Orbit:</b> Polar</p> <p><b>Station:</b> NASA (Alaska), Commercial (Kongsberg Satellite Service – Norway and Swedish Space Corporation – Alaska), Partner (NOAA)</p>
<b>AURA</b>	 <p>Obtains measurements of ozone, aerosols and key gases throughout the atmosphere using innovative instrumentation. Scientists use these data to gain revolutionary insights into the chemistry of our atmosphere.</p>	<p><b>Orbit:</b> Polar</p> <p><b>Station:</b> NASA (Alaska, Wallops) Commercial (Kongsberg – Norway and Swedish Space – Alaska), Partner (NOAA – Alaska)</p>
<b>Orbiting Carbon Observatory - 2</b>	 <p>Comprised of a single instrument that acquires space-based global measurements of atmospheric carbon dioxide with the precision and resolution needed to identify and characterize the processes that regulate this important greenhouse gas.</p>	<p><b>Orbit:</b> Polar</p> <p><b>Station:</b> NASA (Alaska) Commercial (Swedish Space – Alaska)</p>

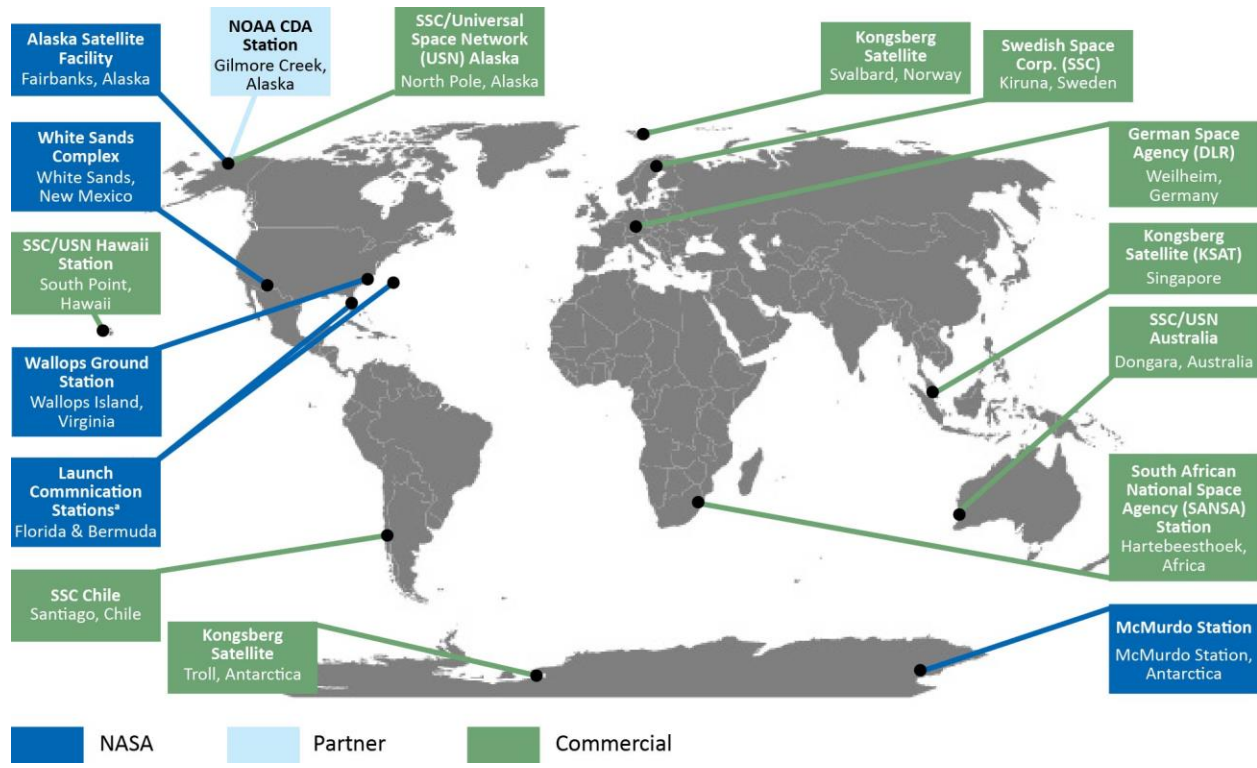
Source: NASA.

The Near Earth Network uses four NASA-owned ground stations, three in the United States – on the campus of the University of Alaska, in Fairbanks; on the Wallops Flight Facility (Wallops) in Virginia; and on the White Sands Complex (White Sands) in New Mexico – and one at the McMurdo Station in Antarctica. At the time of our audit, NASA was expanding the Network’s capacity by installing new antennas at the Kennedy Uplink Station at Kennedy Space Center and at the Ponce de Leon Ground Station in New Smyrna Beach, Florida. A portion of this new capacity will be dedicated to supporting the launch activities for the vehicles NASA intends to use to send humans into deep space – the Space Launch System (SLS) and Orion Multi-Purpose Crew Vehicle (Orion). NASA also installed a third antenna at the Fairbanks facility, which became operational in July 2014.

As NASA works towards commercializing communication with a goal of reducing costs, the Near Earth Network supports its mission set with a mixture of NASA-owned stations, other Federal Government agencies, and domestic and foreign commercial service provider stations. The Agency maintains agreements for services with its Federal Government partners, as well as the commercial entities. For example, the Network uses antennas and transmitters owned by Kongsberg Satellite Services, and Swedish Space Corporation and its subsidiary – Universal Space Network. In 2015, the Network used

Kongsberg’s Norway and Antarctica stations and the Universal Space Network’s station in North Pole, Alaska for almost 30 percent of the 150 daily communications “passes” – when an antenna makes contact with an orbiting spacecraft and data is transmitted – the Network provided to customers that year.<sup>4</sup> The Network also uses antennas and transmitters owned by NOAA as an emergency contingency backup for a limited mission set (see Figure 3).

**Figure 3: Locations from which NASA Obtains Communication Services**



Source: NASA.

Note: NOAA CDA refers to National Oceanic and Atmospheric Administration Command and Data Acquisition, which the Network uses for emergency contingency backup for a limited mission set.

<sup>a</sup> Planned stations.

<sup>4</sup> In 2014, the Network supported about 47,000 passes and estimates that by 2021 it will support an average of about 59,000 passes annually.

# Organizational Reporting Structure of the Near Earth Network

---

While the Headquarters-based SCaN Program provides programmatic direction to the Near Earth Network, the Network's Project Office resides at Goddard Space Flight Center (Goddard) and reports through Goddard's Exploration and Space Communications Projects Division to the Center Director.

**Goddard Space Flight Center.** Goddard provides the Network with personnel, facilities, and independent review services and is responsible for assuring Network activities are conducted in accordance with Agency and Center requirements.

**Project Manager.** The Network Project Manager is responsible for the safety, technical integrity, performance, and success of the Network and for meeting cost and schedule commitments. The Project Manager reports to both the SCaN Program and to Goddard management. The Project Manager manages and executes Network activities according to direction from the SCaN Program.

**Contractor and Subcontractors.** In October 2008, Goddard awarded a cost-plus-award-fee contract to Exelis, Inc., (Exelis) to operate and maintain the Near Earth Network by using a mix of NASA assets and commercial entities.<sup>5</sup> Exelis is responsible for managing NASA-owned Network assets, providing pre-mission coordination and testing with customers, implementing sustainment and development efforts, and awarding subcontracts to commercial entities for additional communications services. The contractor also operates the Agency's antennas at Wallops, White Sands, and McMurdo and subcontracts with the following entities for other services.

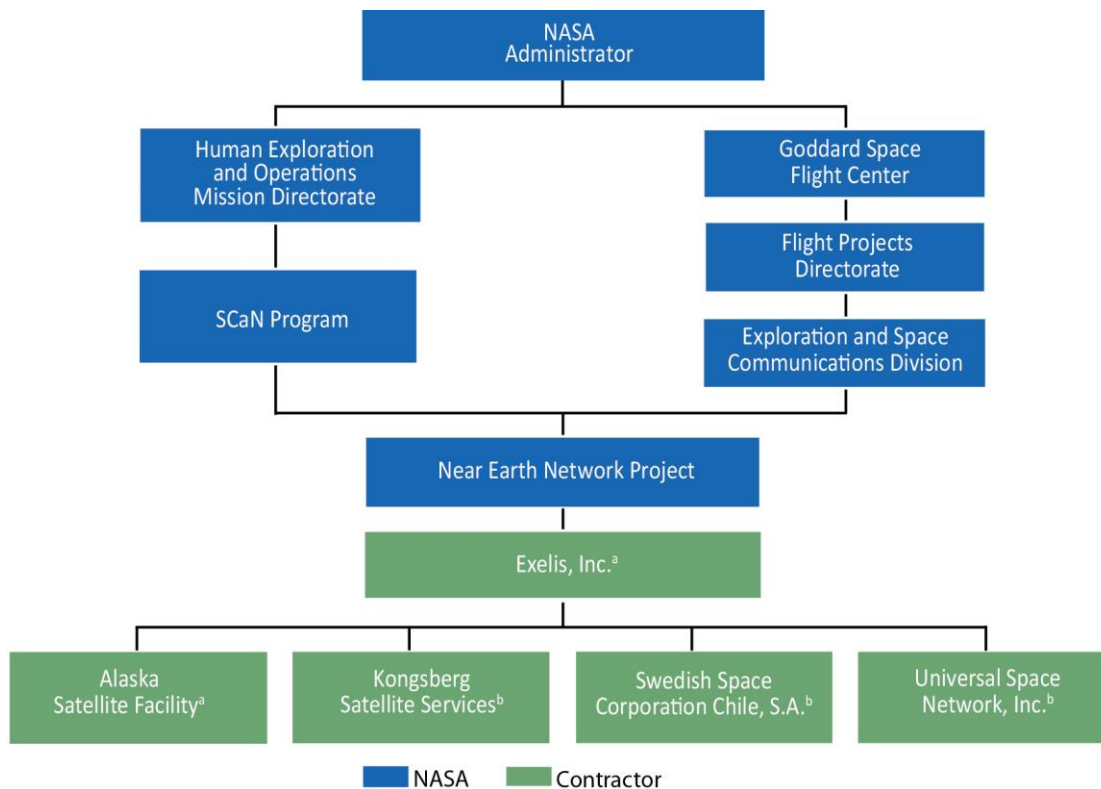
- *Alaska Satellite Facility.* Alaska Satellite Facility provides personnel, materials, and equipment to operate the NASA-owned antennas and systems located in Fairbanks, Alaska. The current cost reimbursable subcontract began in 2011, and extends to June 2016.
- *Kongsberg Satellite Services.* Kongsberg Satellite Services is a commercial company partially owned by the Norwegian Ministry of Trade, Industries, and Fisheries. Kongsberg provides services from antennas located at Troll, Antarctica; Svalbard, Norway; and Seletar, Singapore. The current subcontract began in 2011, and NASA pays a fixed price per pass.
- *Swedish Space Corporation.* Swedish Space Corporation, which is owned by the Swedish Government, provides services from an antenna located in Santiago, Chile and Kiruna, Sweden. The current subcontract began in 2011, and NASA pays a fixed price per pass.
- *Universal Space Network, Inc.* Universal Space Network provides services from antennas located at North Pole, Alaska; South Point, Hawaii; and Dongara, Australia. The current subcontract began in 2011, and NASA pays a fixed price per pass. Until July 1, 2015, Universal Space Network operated as an independent business operation from its parent company, the Swedish Space Corporation, but since then has become a division of the Space Corporation's Satellite Management Services Organization.

---

<sup>5</sup> The contract was originally awarded to ITT Corporation. In 2011, ITT separated into three independent companies, one of which was Exelis, Inc., a global aerospace, defense, information, and services company. In 2015, Harris Corporation acquired Exelis.

Exelis also monitors subcontractors' performance and compliance with Network procedures. See Figure 4 for the organizational structure of the Near Earth Network.

**Figure 4: Near Earth Network Organizational Reporting Structure**



Source: NASA OIG analysis of Network data.

<sup>a</sup> Cost plus contract.

<sup>b</sup> Fixed price contract.

## Information Technology and Physical Security Management of Network Assets

The Near Earth Network relies heavily on secure and well-functioning information technology (IT) systems to ensure continued communications and command and telemetry support. Like all IT-reliant systems, the Network is susceptible to cyber-attack. In 2011, the U.S.-China Economic and Security Review Commission reported four separate instances consistent with cyber activity on the command and control systems utilized by the Network, and in two of these instances, the attacker gained sufficient access to issue commands to satellites, but stopped short of actually doing so.<sup>6</sup>

<sup>6</sup> U.S. Government Printing Office, "2011 Report to Congress of the U. S. – China Economic and Security Review Commission," November 9, 2011, [www.uscc.gov/sites/default/files/annual\\_reports/annual\\_report\\_full\\_11.pdf](http://www.uscc.gov/sites/default/files/annual_reports/annual_report_full_11.pdf) (last accessed on March 14, 2016).

## Legislative Authority and Guidance for IT and Physical Security

The Federal Information Security Modernization Act (FISMA) of 2014 and the Homeland Security Act of 2002 provide guidance to Federal agencies regarding securing Federal information systems, data, and physical infrastructure.<sup>7</sup> FISMA requires agencies to develop, document, and implement agency-wide programs to provide security for the information and related systems that support their operations and assets. The Department of Homeland Security is responsible for developing physical security standards for Federal agencies, facilities, and infrastructure. To help implement FISMA, the National Institute of Standards and Technology (NIST) developed a standard risk management framework.<sup>8</sup> Employing effective and risk-based processes, procedures, and technology helps ensure information systems have the resilience to support ongoing Federal responsibilities, critical infrastructure applications, and continuity of Government.

The NIST framework includes:

- *Categorization of Information Systems and Selection of Security Controls* – to build information security capabilities into Federal information systems through the application of state-of-the-practice management, operational, and technical security controls.
- *Implementation and Assessment of Security Controls* – to maintain awareness of the security state of information systems on an ongoing basis through enhanced monitoring processes.
- *Authorization of the Information Systems and Monitoring of Security Controls* – to provide essential information to senior leaders to facilitate decisions regarding the acceptance of risk to organizational operations and assets.

A summary of the NIST framework and associated Federal and NASA guidance can be found in Appendix B.

NASA adopted NIST standards and Homeland Security Act guidelines, and the Agency's Office of Chief Information Officer (OCIO) and Office of Protective Services (OPS) work together to ensure alignment of security objectives and to develop Agency policies and guidelines.<sup>9</sup> The OCIO is responsible for developing and maintaining an Agency-wide information security program and ensuring the Agency complies with applicable Federal and NASA information security requirements. In addition, the OCIO's Communications Services Office provides computer network services for missions and projects and some centralized IT security continuous monitoring services through the NASA Communications (Nascom) Mission Network.<sup>10</sup> The Center Chief Information Officer (CIO) is responsible for executing the responsibilities of the OCIO at the Center level.

---

<sup>7</sup> FISMA Pub. L. No. 113-283, 128 Stat. 3073 (2014). For the Homeland Security Act, see: Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (2002).

<sup>8</sup> Federal Information Processing Standards (FIPS) publications and the supporting NIST 800-series of special publications.

<sup>9</sup> NASA Procedural Requirements (NPR) 1600.1A, "NASA Security Program Procedural Requirements," August 12, 2013.

<sup>10</sup> NIST defines information security continuous monitoring as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. Nascom Mission Network data connectivity and transport services allows for remote management of various NASA computer services such as centrally managed security tools and end user operating system updates.

The OCIO and OPS have partnered to form the NASA Critical Infrastructure Protection Program through which they implement enhanced security measures for critical infrastructure. OPS has responsibility for conducting assessments for the Protection Program and coordinates with the OCIO and Center CIO to ensure critical cyber assets are identified and included in the Agency's critical infrastructure inventory.<sup>11</sup>

As part of the Protection Program, NASA developed policies addressing physical security for critical infrastructure.<sup>12</sup> These policies assist Agency organizations in identifying and prioritizing protections for their assets and require them to designate facilities at one of four Facility Security Levels. NASA policy requires critical infrastructure carry at least a Facility Security Level III designation and organizations to consider all available funding sources to implement security-related efforts.

**Goddard's Role in Security Management of the Near Earth Network.** Goddard's IT and Communications Directorate (ITCD) utilizes the Nascom Mission Network to provide IT security services and the Center's OPS provides physical security for the Near Earth Network.<sup>13</sup> The Center also applies NASA's common control structure for managing IT security, which includes intrusion detection and prevention, malware protections, vulnerability scanning, and applying and monitoring security configurations.<sup>14</sup> In cases where the Agency's common control cannot be applied due to technical incompatibility, network boundary protections, or other reasons, each individual project or mission system must test and apply the control internally in a coordinated effort between Goddard's ITCD and OPS, the Communications Services Office, and the respective system.

**Contractual Security Requirements.** NASA's contract with Exelis requires the contractor to follow the most recent versions of NASA's IT and physical security policies and associated procedures.<sup>15</sup> In addition, Exelis requires subcontractors to meet the standards in NASA's Information Security Policy and the Agency's IT Security Handbooks.

---

<sup>11</sup> Critical infrastructure are operations, functions, physical assets, or IT resources essential to the success of the Agency's mission. Until 2013, the Agency referred to critical infrastructure as "mission essential infrastructure."

<sup>12</sup> NPR 1600.1A; NPR 1620.2, "Facility Security Assessments," October 4, 2012; and NPR 1620.3, "Physical Security Requirements for NASA Facilities and Property," October 4, 2012.

<sup>13</sup> Goddard's CIO resides within the Center's ITCD.

<sup>14</sup> NASA common controls are controls that can be applied to NASA systems connected to the Agency's institutionally managed networks. Many of these security controls are automated controls applied using software agents that reside on end user components.

<sup>15</sup> The contract states Exelis shall implement a compliant IT Security Program, which meets at least the minimum requirements of the NASA IT Security Program as specified in the most current editions of NASA Policy Directive (NPD) 2810.1 "Security of Information Technology," NPR 2810.1, "Security of Information Technology," and NASA Federal Acquisition Regulation Supplement 1852.204-76, "Security Requirements for Unclassified Information Technology Resources."

# NETWORK SECURITY MANAGEMENT NOT COMPLIANT WITH REGULATIONS AND LACKS NECESSARY ELEMENTS FOR EFFECTIVE SECURITY

NASA, Goddard, and the Near Earth Network Project Office deviated from and failed to consider fundamental elements of Federal and Agency IT and physical security risk management policies and standards for protecting the Network. Specifically, the security categorization NASA assigned to the Network does not reflect its mission-essential nature and the Agency did not include the Network in its Critical Infrastructure Protection Program; external information system connections are not being managed in accordance with Federal and Agency policy; technical security controls are not in place or functioning as intended; and physical security controls have not been implemented on NASA-owned and supporting contractor facilities in accordance with Federal or Agency standards. These deficiencies increase the likelihood that the Network's IT and physical infrastructure are susceptible to compromise.

## Network Not Protected as Mission-Essential Infrastructure

---

NASA assigned a security categorization rating of "Moderate" to the Near Earth Network and did not include the Network in its Critical Infrastructure Protection Program. We believe this categorization was based on flawed justifications and that the Network's exclusion from the Protection Program resulted from a lack of coordination between Network stakeholders. Given the importance of the Network to the success of NASA Earth science missions, the contingency support it provides for the Space Network, and the plans for it to support human space flight in the future, we believe a higher categorization rating and inclusion in the Protection Program is warranted.

## NIST Categorization Guidance

NIST's Risk Management Framework categorizes an information system based on the information the system processes, stores, and transmits as well as the potential impact an event would have if the confidentiality, integrity, or availability of that information was compromised.<sup>16</sup> Information systems are categorized as "High," "Moderate," or "Low" after determining the highest mark assigned to any one of the elements. For instance, if the impact level of just one of the elements is determined to be high then the system is categorized as "High." The final impact determination is based on the potential impact to an organization should certain adverse events occur that would jeopardize the information and systems the organization needs to accomplish its mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. NIST has developed

---

<sup>16</sup> The loss of confidentiality is the unauthorized disclosure of information. The loss of integrity is the unauthorized modification or destruction of information. The loss of availability is the disruption of access to or use of information or an information system.

guidelines recommending the types of information and systems included in each category, the minimum-security requirements for each category, and the recommended controls. The higher the security categorization, the more stringent the NIST-recommended security controls will be. In other words, a categorization of “High” will require an organization to implement more and stronger security controls.

Among the information types identified by NIST is “Space Operations,” which is characterized by the need to maintain integrity and availability of communications during critical events, such as commanding spacecraft. NIST recommends a provisional security impact level of “High” for systems that process Space Operations-type information.

## Near Earth Network’s Categorization

Goddard’s ITCD and Network personnel categorized the Near Earth Network as processing the Space Operations-type information; however, they deviated from the provisional NIST recommendation of a “High” security categorization. In our judgment, this deviation does not accurately reflect the significance of the Network’s role in supporting missions for NASA.

Agency IT security personnel downgraded the integrity objective of the categorization to “Moderate” using the justification that the Network provides only throughput of data – meaning that data and commands do not reside on Network systems and Network components are used only as a conduit to transmit data and commands between the mission on the ground and the spacecraft. However, we believe the Network is more than a simple conduit for communications and the downgrade to “Moderate” for the integrity objective was inappropriate. Network components must store (albeit temporarily) and process data and commands prior to transmitting to the spacecraft.<sup>17</sup> If any step in the transmission process is interrupted, whether by equipment malfunction, environmental interference, or intentional manipulation, it could affect the integrity of the data and commands being sent to or received from the spacecraft.<sup>18</sup>

Agency IT security personnel also downgraded the availability objective to “Moderate,” with the only justification provided relating to the status of an antenna owned by Wallops that is not part of the Network’s infrastructure but is sometimes used as a backup.<sup>19</sup> However, the justification did not explain why the downgrade was appropriate for other antennas and equipment the Network uses regularly. See Table 1 for a summary of the Network’s determination matrix for the information type Space Operations.

---

<sup>17</sup> Network components process satellite transmissions by modulating and or demodulating and ensuring appropriate frequencies, channels, and timing sources are utilized.

<sup>18</sup> For example, erroneous frequency assignment information could result in loss of communications or a distributed denial of service attack could prevent a signal from reaching its target.

<sup>19</sup> Further inquiry revealed the Network no longer uses this particular antenna.



**Table 1: Security Categorization Determination Matrix for Near Earth Network**

<b>Information type:</b> D11 – Transportation		
<b>Information sub-type:</b> D11.4 – Space Operations		
<b>Confidentiality Impact Level</b>	<b>NIST:</b> Low	<b>Network:</b> Moderate
Justification for any deviation from the NIST recommended impact level	Command uplinks are restricted to the mission and most command data formats are not publicly available	
<b>Integrity Impact Level</b>	<b>NIST:</b> High	<b>Network:</b> Moderate
Justification for any deviation from the NIST recommended impact level	Stations provide throughput only and has no command insight	
<b>Availability Impact Level</b>	<b>NIST:</b> High	<b>Network:</b> Moderate
Justification for any deviation from the NIST recommended impact level	The Wallops Range 7.3 meter antenna is used for back up only	

Source: NASA OIG presentation of information from System Security Plan for the Near Earth Network (MEI) SO-002-M-GSF-4013 - (Derived from NIST Standard Publication 800-60).

Given the importance of the Network to the success of many NASA Earth science missions, the launch and contingency support it provides other Federal agencies, and plans for it to support human space flight, we believe that it should be categorized as “High,” and that the additional security controls accompanying such a designation should be implemented.

We also believe the Near Earth Network has many of the characteristics of critical infrastructure. NASA defines infrastructure as critical if its “damage or destruction would have a debilitating impact on the ability of NASA to perform its essential functions and activities.” The Network provides critical command, telemetry, and communications support to more than 40 science missions at the Agency and damage to the Network could have a debilitating impact on these missions. In addition, the Network provides contingency support for NASA’s Space Network satellites and is one of several providers for launch and early orbit and contingency support for NOAA’s National Environmental Satellite, Data, and Information Service Program satellites, which provide weather forecasting for the United States – itself an essential function.<sup>20</sup> Moreover, both the Network System Security Plan and Space Communication Network Services Security Management Plan refer to the Network as mission essential or critical infrastructure.

Goddard’s OPS, ITCD, and Network personnel failed to coordinate regarding categorization of the Network and its inclusion in NASA’s Protection Program. According to Federal and NASA policy, to be considered for NASA’s Protection Program an asset would (1) have an impact on essential NASA missions and the loss or compromise of the asset could enable a hostile entity to disrupt or otherwise threaten the ability of NASA to satisfy its essential missions; (2) be required for NASA’s mission capability; (3) be integral to the performance of NASA’s mission, have a very large dollar value, or be difficult or impossible to replace in a reasonable period of time; and (4) be a system other agencies depend on to accomplish their essential missions serving the general public. In our judgment, the Network performs critical space operations and meets all of the criteria for inclusion in the Protection Program. Had Goddard’s OPS, ITCD, and Network personnel worked together to correctly categorize the

<sup>20</sup> NOAA considers the National Environmental Satellite, Data, and Information Service Program a primary mission essential function and has categorized its associated ground stations as “High” impact for security purposes.

Network as “High” and included its assets within the Protection Program, the Network would have received more robust IT and physical security controls, including improved monitoring, intrusion detection, and electronic physical access controls.

## **NASA Lacks Visibility of the Security Posture of the Network’s External Information System Connections**

---

The Near Earth Network maintains connections to the systems of four external organizations that process and store Agency data using either NASA-owned or their own equipment.<sup>21</sup> The Network has external information system security interconnection agreements with each of these entities. However, we found because NASA is not managing these agreements in accordance with Agency and Federal policy, it lacks visibility into the security posture of the external information systems.

NASA’s policy on security management of external information systems includes requirements to ensure information processed by non-Agency systems is safeguarded. Specifically, Agency policy directs programs and projects to identify external systems and assess the security posture of these systems on a continuous basis.<sup>22</sup> Security risks or problems should be corrected or addressed in a timely manner, corrective actions documented, and associated records stored in a secure location. During our audit, NASA’s OCIO was developing clearer procedures to address NASA and Federal requirements for assessing external systems and ensuring an appropriate level of assurance.<sup>23</sup>

The Near Earth Network System Security Plan, dated August 30, 2012, requires external system interconnections to adhere to NASA’s IT and physical security standards. Although NASA identified the Network’s interconnections as external systems in the Security Plan, interconnection agreements with the commercial entities were not created until May 2015. Further, as of February 2016, the Agency had not performed a formal security assessment of these external systems, and we identified weak or missing security controls on our visits to the Alaska Satellite Facility and Universal Space Network’s North Pole Ground Station Facility. This occurred due to ineffective oversight during the Network’s most recent Assessment and Authorization cycle and an overall lack of awareness of Network operations and assets by the responsible Network and Goddard ITCD personnel.<sup>24</sup> In addition, until recently NASA did not have clear guidance in place for managing the security of external system connections. Without formal assessments or reporting, NASA has little visibility into the security posture of the interconnected systems and cannot ensure the owners of those external systems can adequately prevent, detect, respond, or report security events.

---

<sup>21</sup> The University of Alaska, Kongsberg Satellite Services, Swedish Space Corporation, and Universal Space Network.

<sup>22</sup> NIST policy permits security reviews by designated audit authorities of one or both organizations or by an independent third party.

<sup>23</sup> The new guidance includes a checklist for a Security Assessment Team to obtain a risk understanding of any changes to the external information system and verify the system’s security posture since the last assessment.

<sup>24</sup> NASA’s Assessment and Authorization cycle is part of the risk management process and an integral part of the Agency’s information security program. It is essential that an information system’s Authorizing Official has sufficient information regarding the security posture of their system to make the appropriate risk based decision on whether to authorize or deny the operation of the system.

## Inadequate Continuous Monitoring of the Network

---

Continuous monitoring refers to maintaining an ongoing awareness of computer networks, which includes dedicated staff, automated tools to detect and respond to suspicious activity, and a formal security incident reporting process. We found security baseline configuration application and monitoring, vulnerability identification and mitigation, malicious code protections, and event and incident management capabilities, which are components of the continuous monitoring of the Near Earth Network were lacking or not operating as intended. This resulted from a failure to coordinate between Network personnel, Goddard's ITCD, and the Communications Services Office, as well as a lack of understanding of security policies. As a result, the Network is not best positioned to effectively identify or respond to vulnerabilities or malicious activity.

### Security Configuration Baseline Application and Monitoring

Components of the Near Earth Network did not have properly applied or monitored security configuration baselines, which left the Network less secure, more prone to compromise, and lacking useful information to respond to a cyber-attack. This happened because the Network's Information System Owner made the decision not to install NASA-recommended monitoring software on its components due to interoperability issues on Network systems, and Network system administrators were unclear about how to accomplish continuous monitoring using other processes.<sup>25</sup> Without this control, or other compensating measures, the Network is less secure.

The Office of Management and Budget has directed Federal agencies to apply secure configuration baselines on federally-owned and contractor-operated systems. Security configuration baselines refer to a group of configuration settings used to harden components and help monitor for unusual activity that could indicate malicious activity is taking or has taken place. To support this requirement, NASA's OCIO developed guidance for the application of security configuration baselines for systems that process and store Agency data.<sup>26</sup>

Security configuration baselines are applied to NASA's systems via KACE software.<sup>27</sup> However, due to interoperability issues on the Near Earth Network, the Network's Information System Owner decided to not install the KACE software. Notwithstanding, the Network was still responsible for implementing and monitoring applicable security configuration baselines internally. Although Network system administrators install an initial security configuration baseline before components are put in service, these baseline configurations do not meet Agency security configuration standards and therefore do not provide the same level of continuous monitoring capabilities, which leaves Network components unnecessarily susceptible to compromise. Similar to a finding in our report on the Deep Space Network, we noted that Near Earth Network system administrators were unfamiliar with NASA's security configuration baseline standards.<sup>28</sup> In our judgment, the Network is introducing unnecessary risk by not applying and monitoring NASA's security configuration baselines on Network components.

---

<sup>25</sup> The Information System Owner ensures implementation of all Agency and Center requirements at the system level and that security controls are implemented according to a thorough risk-based analysis of their information systems' security posture.

<sup>26</sup> The NASA Agency Security Configuration Standards office develops NASA policy and content for the application of security configuration baselines for NASA system components.

<sup>27</sup> KACE is a NASA-owned software suite used for ensuring compliance with NASA security configuration guidelines.

<sup>28</sup> NASA OIG, "Audit of NASA's Management of the Deep Space Network" (IG-15-013, March 26, 2015).

## Vulnerability Identification and Mitigation

Vulnerability identification and mitigation practices of Goddard and Near Earth Network staff are not comprehensive or effective leaving Goddard's ITCD without adequate visibility into Network components. Poor vulnerability management practices can lead to undetected vulnerabilities residing on the Network, inadvertent exclusion of components, and component failures. In our judgment, the poor practices occurred because of a lack of coordination between responsible Network personnel and Goddard's ITCD.

NIST guidance directs organizations to run vulnerability-scanning tools on all network systems and deliver prioritized lists of the most critical vulnerabilities to system administrators. Agencies should perform vulnerability scanning in an authenticated or credentialed mode, which identifies critical vulnerabilities residing on a system or network not revealed by non-credentialed scans.<sup>29</sup> NASA requires non-credentialed vulnerability scans on Agency systems monthly and credentialed scans on a quarterly basis. The Agency also requires identified vulnerabilities be remediated in a timely manner.

Similar to findings in our report on the Deep Space Network, the Near Earth Network is performing limited scanning but not the required quarterly credentialed scans.<sup>30</sup> According to the Network's System Security Plan, Goddard's ITCD is responsible for performing scanning on all applicable Network components. While Goddard's ITCD performs quarterly non-credentialed scans as a standard service, the Network has not requested credentialed scanning.

Network system administrators told us that vulnerability-scanning procedures have led to some Network components crashing and disruptions with missions losing communications support. System administrators also provided a discrepancy report identifying six separate occasions between January and May 2015 when components crashed and remained down for as long as 20 minutes. We determined crashes occur because some Network components have limited functional capability, lack internal resources (such as computer memory), or do not contain an operating system. Because of these characteristics, vulnerability scanning is likely to disrupt operations. NASA's IT Security Handbooks outline a process for avoiding these problems during vulnerability scanning, including allowing IT security personnel to request temporary exceptions from vulnerability scanning when it threatens to negatively impact or render an information system unusable. However, the Network was unaware of these exceptions and did not seek to resolve them with Goddard's ITCD.

While the Network relies on Goddard's ITCD to provide quarterly scanning services, we believe ITCD lacks visibility into much of the Network's infrastructure. For example, until our audit, the Network did not realize ITCD had not scanned 42 components located at foreign sites and ITCD was not aware the

---

<sup>29</sup> Credential scanning is crucial because the scanner authenticates the systems components and obtains detailed information about installed applications including missing security patches. In contrast, non-credentialed scans are less comprehensive and have more false positives. A good analogy to contrast the two types of scans is the approach a mechanic may take in assessing a car. A mechanic may assess the car by looking at the exterior, kicking the tires, and listening to the motor. While this may be useful in some cases, there is much more information to be obtained by opening the hood and inspecting the car's engine.

<sup>30</sup> In our 2015 audit of the Deep Space Network, credentialed scanning was not being performed on its systems and system administrators were unaware of the requirement to do so. During the audit, we requested to perform credentialed scanning on a sample of 74 components. The credentialed scans identified 126 critical vulnerabilities, which could potentially be exploited resulting in complete takeover of the host operating system, and more than 1,000 high-impact vulnerabilities, any of which have the potential to allow malicious activity on the affected system.

foreign sites existed. Without greater coordination, increased scrutiny of scan results, and a more comprehensive understanding of the Network's IT system components, locations, and required credentials, Goddard's ITCD cannot effectively enforce scanning requirements on all Network components, therefore increasing the chances of undetected and unmitigated vulnerabilities.

## Malicious Code Protections

The Near Earth Network does not have an effective way to ensure malicious code (malware) protections are in place and operating as intended. NASA policy requires malware protection tools be automatically updated with new software releases.<sup>31</sup> The Network relies on Goddard's ITCD to update malware protection to end users automatically. However, Network personnel told us that because of extended server crashes they have not utilized malware protection software at Wallops or other sites. Furthermore, we found that anti-malware signatures in the protection software had not been updated since the beginning of 2015.<sup>32</sup> As a result, the Network has no automated technical controls for detecting or preventing the effects of malware if a Network system component becomes infected. Goddard's ITCD told us they were unaware of any issues with server crashes and that to their knowledge no other project or mission has experienced loss of services due to server crashes. In our judgment, this issue further illustrates the lack of coordination between responsible parties, which prevents timely resolution of problems affecting the Network's security posture.

## Event and Incident Management

The Near Earth Network's event and incident monitoring capabilities do not allow capture of sufficient activity, which prevents a thorough analysis of anomalies and therefore leaves significant security gaps in the Network's infrastructure. This resulted from Network officials interpreting Nascom Mission Network policy to prohibit the installation of monitoring software.

NIST recommends organizations implement an event and incident management capability that involves monitoring and responding to observable occurrences in a network or system. A variety of tools and technologies exist to monitor events, such as intrusion detection systems and logging mechanisms. Some tools may detect events based on known attack signatures, while others detect anomalies in behavior or performance that could indicate an attack. Certain events, such as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices, may signal that an incident has occurred. Incident management tools may assist in detecting, responding to, and limiting the consequences of a malicious cyber-attack against an organization.

We found the Network's event and incident management capabilities do not include a strategy for auditing, logging, intrusion detection, or packet capture capabilities.<sup>33</sup> While the Network directs

---

<sup>31</sup> Malware detection provides the ability to identify the presence of viruses, Trojan horses, spyware, or other malicious code on or destined for a target system transported by electronic mail, electronic mail attachments, Web accesses, removable media, or inserted through the exploitation of information system vulnerabilities. NASA IT Security Handbook ITS-HBK-2810.14.01, "System and Information Integrity," December 1, 2014.

<sup>32</sup> Anti-virus/malware signatures are unique values that indicate the presence of malicious code. When an anti-virus program scans a computer, it calculates the signature for a file and compares that signature to a list of known bad signatures. If the scan identifies a match, the software will take the necessary steps to quarantine or remove the identified malware.

<sup>33</sup> Auditing certain events that transpire on a machine enables a complete picture of activity leading up to an event. For example, the Network should store those auditable events, and monitor or review the network traffic leading up to the event.

ground station operators to utilize a discrepancy system to report anomalous activity affecting communications passes, we found this system does not allow adequate analysis to determine the root cause of anomalous activity. For example, the Network provided a list of almost 700 instances of system anomalies occurring in FYs 2014 and 2015, including equipment failure, lost communications, and times when orbital pass support was prevented. Many times, these events were simply corrected after a system reboot but remained open in the discrepancy reporting system because the Network could not determine an exact cause. Our review of some of these anomalies identified questionable activity that could indicate cyber intrusion, including large dumps of junk data that overloaded component resources, messages indicating file sharing violations, unresponsiveness to commands, and other erratic behavior. However, because the Network does not effectively capture forensic information for further analysis and does not own or use any IT security tools, NASA is unable to determine if the problem was the result of a component malfunction, environmental interference, or an intentional malicious effort to disrupt communications.

The Network does not have a strategy for comprehensive auditing, logging, intrusion detection, or packet capture capabilities for its components because Network officials interpreted Nascom Mission Network's policy to prohibit them from installing monitoring software. However, according to Goddard ITCD personnel, the policy was intended to prohibit personnel from installing monitoring software on components within the Nascom Mission Network's boundary, not to prohibit the Network from installing incident and monitoring software on its own components.

In an effort to benchmark anomaly management with the practices of one of the Agency's Federal partners, we requested information related to NOAA's anomaly reporting process for its National Environmental Satellite, Data, and Information Service Program. NOAA's guidance states that anomalies relating to satellite and ground system operations shall be reported to its Deputy Assistant Administrator with copies to the Assistant Administrator, Deputy Assistant Administrator for Systems, the CIO, and the Agency's Chief of Staff. Further, a reportable anomaly that constitutes an IT security incident must also be reported through existing NOAA IT security procedures.

By comparison, the Near Earth Network's anomaly reporting procedure does not require Network operators to report anomalies that may constitute an IT security incident to NASA's Security Operations Center (SOC).<sup>34</sup> Further, there is no mention of the role of ITCD in the discrepancy reporting procedures. Coordination between the Network, Goddard's ITCD, and the SOC helps to ensure NASA is meeting its reporting requirements to the United States Computer Emergency Readiness Team while also better investigating anomalous activity on critical NASA communications systems.<sup>35</sup> Without an improved anomaly management capability, the Network is unable to capture sufficient information on system anomalies for a thorough analysis, thereby leaving significant security gaps in Network infrastructure.

The key elements of a comprehensive continuous monitoring program include security baselines, vulnerability identification and mitigation, malware protections, and event management and incident response capabilities. While NASA has the appropriate IT security tools and resources available,

---

<sup>34</sup> The SOC is responsible for monitoring Agency network traffic for suspicious activity and performing any needed investigation. It is located at Ames Research Center, and operates continuously with 39 dedicated IT security personnel.

<sup>35</sup> The United States Computer Emergency Readiness Team is part of the U.S. Department of Homeland Security's National Cybersecurity and Communications Integration Center. The Team leads efforts to improve the Nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks to the Nation. Federal agencies are required to report cybersecurity incidents to the Team within strict timeframes.

individual programs must ensure that these capabilities are in place and functioning as intended. Without these capabilities functioning effectively, both the Network and NASA are at risk of operating in a compromised environment.

## Physical Security Controls Not in Compliance with Federal and NASA Policies

---

Physical security controls for the Near Earth Network and supporting contractor facilities do not meet Federal or Agency policies. This occurred because of insufficient coordination between the Network, Goddard, and NASA's OPS. As a result, OPS was not aware of Network or supporting contractor facilities and was unable to enforce appropriate safeguards, leaving the Network unnecessarily vulnerable to compromise.

### Review of Key NASA Facilities

Federal agencies are required to establish a program to identify critical infrastructure and key resources, evaluate assets for vulnerabilities, and fund and implement appropriate security enhancements to mitigate vulnerabilities. NASA policy states facilities designated as communications ground stations or data centers shall be rated and protected at a minimum level of Facility Security Level III, which mandates controlling access through the use of intrusion detection systems, electronic physical access control systems, and closed circuit television. NASA's OPS serves as the focal point for policy formulation, oversight, coordination, and management of the Agency's security services and protection of NASA assets.

**Network Equipment at Wallops.** Network antennas at Wallops did not have perimeter protections required for Facility Security Level III facilities. Specifically, the antenna structures and connected equipment were not protected by fencing, intrusion detection system, or electronic physical access control systems. Goddard and Wallops OPS personnel told us that prior to our audit they were not fully aware of the Network and the services it provides. After our audit was announced, Wallops OPS initiated a security assessment of on-site Network assets to bring them into compliance with a Facility Security Level III rating. OPS completed the assessment in May 2015 and made numerous recommendations that were pending implementation as of publication of this report. However, the assessment did not include the antenna apertures and supporting equipment enclosures at Wallops, which are vital components of the Network. When we discussed the omission of these facilities with Wallops OPS officials, they stated that a waiver for fencing around antennas will likely be submitted due to funding constraints.

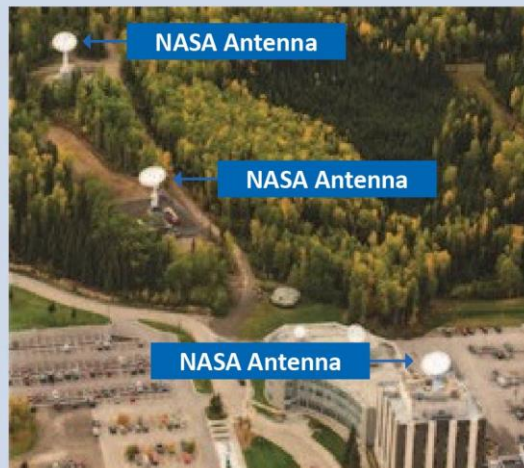
**Wallops 11-Meter Antenna**



Source: NASA.

**NASA Equipment at Alaska Satellite Facility.** NASA assets at the Alaska Satellite Facility are also not being protected as required by NASA and Federal policies. In addition to Network equipment, we found the Facility houses one of NASA’s Earth Observing System Data Information System Distributed Active Archive Centers, which are used to process, archive, document, and distribute data from the Agency’s past and current Earth-observing satellites and field measurement programs.<sup>36</sup> The Alaska Satellite Facility lacks the required Facility Security Level III designation and the accompanying physical access controls necessary for NASA-owned antennas and systems located at the Facility. Specifically, NASA assets and network infrastructure are not protected with intrusion detection or personal identity verification (PIV) access control.<sup>37</sup> Agency policy requires the performance of a background investigation and a record of the individual in the Agency Identity Management platform alongside access authorization details for specific NASA assets in order for users to access those assets.<sup>38</sup> We found Alaska Satellite Facility personnel had not been vetted through this process. Further, the equipment and antenna areas are not marked with signs for “controlled” or “limited” access areas as required by NASA policy.

#### NASA Antennas at the Alaska Satellite Facility



Source: Alaska Satellite Facility.

**NASA Equipment at Universal Space Network North Pole Facility.** We identified assets supporting the Near Earth Network and Earth Observing System Data Information System Distributed Active Archive Centers at the Universal Space Network’s North Pole Ground Station Facility that are not protected by intrusion detection or PIV access control. NASA policy requires Agency assets, including those located at commercial entities, be protected by these systems. Further, Universal Space Network’s contract with Exelis references the most recent versions of NASA’s IT and physical security policies and requires the protection of Agency assets. SCaN Program officials and Exelis personnel were unaware of NASA’s policies mandating specific physical protections for these assets.

#### Earth Observing System Data Information System



Source: NASA.

<sup>36</sup> The Alaska Satellite Facility has a contract with NASA’s Earth Science Data Systems Program to provide data center management and serve as custodians of Earth observing mission data.

<sup>37</sup> PIV cards are part of NASA’s identity management processes that allow for the proper vetting and authentication before allowing access to NASA systems and data.

<sup>38</sup> NASA’s Identity Management system supports “Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors” and the requisite vetting requirements for personnel with privileged access to NASA facilities, property, systems, and data.



## Joint Work with NASA Headquarters' Office of Protective Services

Headquarters OPS officials accompanied our audit team to Alaska to examine Network assets and agreed with our determination that both the Alaska Satellite Facility and Universal Space Network's North Pole Ground Station Facility were not protected in accordance with NASA and Federal guidance. Specifically, OPS officials identified issues related to NIST controls for system and communications protection, personnel security, physical and environmental protection, media protection, maintenance, system and information integrity, incident response, and access. OPS officials also expressed concern over non-compliance with PIV requirements, but told us that compliance should be relatively easy and inexpensive because NASA's Integrated Services Network infrastructure – a key component for integration into Goddard's electronic physical access control systems – is already in place at each location.

According to Headquarters OPS officials, interconnection agreements between the NASA networks and outside contractor facilities and systems should, at minimum, have detailed, reportable, and measurable requirements. Based on these formal arrangements, contractors should implement agreed upon security policies to augment the security posture of their facilities. While system interconnection agreements exist between NASA, the Alaska Satellite Facility, and the Universal Space Network's North Pole Ground Station Facility, there is little visibility into their security posture and no assessment or reporting mechanisms. This resulted from the Network not following established guidance or ensuring coordination between all Network stakeholders.

# INADEQUATE MAINTENANCE OF GROUND STATIONS COULD INCREASE COSTS

Although the Near Earth Network is performing preventative maintenance on NASA-owned assets, the Network has not been performing or tracking depot-level maintenance on these assets. The failure to perform depot-level maintenance, such as proactively inspecting and replacing cables and mechanical systems that are reaching their failure threshold, could result in unexpected breakdowns of Agency assets and require the Network to purchase more costly commercial services.

## Depot-Level Maintenance Not Performed or Tracked as Deferred Maintenance

Although the Network follows Agency guidance for preventative maintenance of its antennas, the Network does not routinely perform depot-level maintenance or track such maintenance as deferred when it is not performed.<sup>39</sup> NASA has criteria for maintenance and operations for institutional and program facilities and for related equipment to minimize risk to processes, protect and preserve capabilities, and enable Agency missions. For example, NASA requires each Center to develop and monitor an Annual Work Plan that defines all scheduled maintenance. If scheduled maintenance cannot be performed with available resources, the Agency tracks the incomplete maintenance work as deferred maintenance.<sup>40</sup> NASA also requires Centers continuously assess facility conditions to identify and quantify the repairs needed to address the deferred maintenance.<sup>41</sup> Table 2 shows several different maintenance methods utilized at NASA.

**Table 2: Maintenance Types**

Maintenance Type	Description
Depot-Level Maintenance	Take steps to proactively inspect and replace cables and mechanical systems that are reaching their failure threshold and are not addressed by preventative maintenance.
Preventative Maintenance	Scheduled periodic inspection, cleaning, lubrication, and minor repairs at predefined intervals to reduce equipment failures.
Run to Failure	No Maintenance is scheduled or regularly performed to prevent failure.

Source: NASA OIG summary of Agency and Network data.

<sup>39</sup> Deferred maintenance is the total of essential but unfunded maintenance work required to bring facilities and collateral equipment to a condition that meets acceptable standards.

<sup>40</sup> NPD 8831.1E, "Maintenance and Operations of Institutional and Program Facilities and Related Equipment (Revalidated June 17, 2013 w/Change 1)," June 19, 2003.

<sup>41</sup> NPR 8831.2F, "Facilities Maintenance and Operations Management," October 7, 2015.

The Network relies on Exelis to establish a cost effective approach to ensure availability of the Network. While the contractor’s Reliability, Maintainability, and Sustaining Plan (Reliability Plan) establishes the use of preventative maintenance in support of the Network antennas, it does not cover depot-level maintenance. By comparison, Exelis is required to perform depot-level maintenance on Space Network assets. According to Near Earth Network management, with the exception of 2011, the Network has not performed depot-level maintenance since the 1980s.<sup>42</sup> Because depot-level maintenance is not routine and the Network does not identify and track this maintenance as deferred maintenance in the years it is not performed, the Network is operating in a partial “run to failure” strategy. Typically, candidates for “run to failure” are low cost, easily repaired, and non-critical items – labels that do not describe the Near Earth Network.

## Depot-Level Maintenance is Essential to Reliable Ground Station Operations

In 2011, Exelis identified the lack of depot-level maintenance as a risk to the Network, stating that without depot-level maintenance, undetectable mechanical wear could cause an extended downtime failure. This risk was realized in June 2014 when the second oldest antenna at the Alaska Satellite Facility failed due to a broken gear. NASA was fortunate that another antenna was available to enable the Facility to meet mission requirements at no additional cost to the Agency. The Network estimated that had the new antenna not been available, the Alaska facility’s unexpected failure could have forced NASA to move 2,232 communications passes to commercial entities at a cost of \$1.12 million during the 200 days the antenna was out of operation. During the FY 2017 budget development process, Network management noted that depot-level maintenance could have identified the faulty gear prior to the failure.

Broken Gear



Source: NASA.

Growing mission requirements and the addition of new Agency-owned antennas further increases the need for depot-level maintenance. Between 2005 and 2014, the Network’s annual passes increased 7.1 percent to about 47,000, and the Network estimates that by 2021 it will support an average of 12,000 additional passes (25.5 percent more) or about 59,000 passes annually. The Network is also increasingly more reliant on NASA-owned assets to provide those passes rather than using commercial entities. For example, in 2005 the Network supported 63 percent of passes by procuring services from commercial entities. In 2014, the Network’s reliance on commercial entities decreased to 46 percent and the Network is estimating that between 2015 and 2021 commercial entities will supply less than 40 percent of the tracking services on average. Further, NASA will be relying on new antennas the Network is building in Florida to support the SLS and Orion in the coming years.

<sup>42</sup> In 2011, the Near Earth Network completed depot-level maintenance on its antenna at McMurdo. According to Network management, the antenna is one of the Network’s most used antenna and continues to operate at high levels of proficiency following the maintenance.

In spring 2016, the SCaN Program plans to hold an annual operations meeting with all three networks, in which they plan to identify depot-level maintenance best practices. In addition, although the SCaN Program did not approve any of the \$250,000 the Near Earth Network requested in FY 2016 specifically for depot-level maintenance, Program officials said they plan to provide funds for this type of maintenance beginning in FY 2020.<sup>43</sup> While this is a positive step, we also believe the Program should recognize the importance of tracking foregone depot-level maintenance because deferred maintenance data trends can help prioritize maintenance activities.

---

<sup>43</sup> Based on the FY 2016 Consolidated Appropriations Act, the Near Earth Network did not receive more funding than it requested for FY 2016 while the other two Networks will see an increase in their budget (Pub. L. No. 114-113).

# CONCLUSION

The Near Earth Network's ground systems are critical to track and communicate with NASA science missions and will be used to support NASA's SLS and Orion beginning as early as 2018. The success of the Network depends on a global system of antennas and supporting infrastructure that require protection from cyber and physical security threats, as well as maintenance to prevent the failure of Agency assets.

We found that NASA, Goddard, and the Network failed to comply with fundamental elements of security risk management reflected in Federal and Agency policies. We believe that these deficiencies resulted from inadequate Agency oversight of the Network and insufficient coordination between stakeholders. These deficiencies unnecessarily increase the Network's susceptibility to compromise.

We also identified that the Network risks unexpected failures and disruption to vital communications services by failing to conduct depot-level maintenance. This is particularly troubling given the Network's increasing reliance on NASA-owned assets to accomplish its mission. The planned increase in Network usage, coupled with its future use in human space flight, means the Network cannot tolerate extended downtime. The Network should also track deferred depot-level maintenance to help prioritize maintenance in the hopes of minimizing unexpected failures.

# RECOMMENDATIONS, MANAGEMENT'S RESPONSE, AND OUR EVALUATION

To ensure NASA is properly protecting the Network, we recommended NASA's Office of Protective Services, Deputy Associate Administrator for Space Communication and Navigation Program, and Goddard's Office of Protective Services personnel:

1. Include the Near Earth Network in the NASA Critical Infrastructure Protection Program.

To ensure the Near Earth Network's IT security risk management practices comply with Federal and Agency requirements, we recommended NASA's Office of the Chief Information Officer, Deputy Associate Administrator for Space Communications and Navigation, Goddard's Space Flight Center's Information Technology and Communications Directorate, and Network personnel:

2. Recategorize the Network as a "High system" in line with NIST-recommended impact levels and the Network's criticality to mission operations.
3. Review all Network external systems connections to ensure they are maintained in accordance with NIST and NASA guidance and undergo the appropriate level of assessment through the use of NASA's newly developed external systems assessment procedures checklist.

To ensure the Network develops a strategy for continuous monitoring including security controls that comply with Federal and Agency requirements, we recommended Goddard's Information Technology and Communications Directorate and Network personnel:

4. Provide the Network with NASA-procured vulnerability scanning software and train local Network project personnel on its use in accordance with Agency requirements.
5. Implement security baselines to the fullest extent possible on Network systems and assess the baselines for changes on a scheduled basis.
6. Develop a process for reporting compliance with security baselines on Network components.
7. Ensure that malware protections are functioning as intended on applicable Network components.
8. Ensure exemptions requests and IT security waivers are submitted for areas lacking applicable controls.
9. Develop a strategy that at a minimum includes improved event management and incident response capabilities; monitoring and packet capture capabilities at strategically identified ingress and egress points of the Network locations; and an event auditing and logging strategy on all critical Network components.
10. Integrate NASA Security Operations Center incident reporting into Network discrepancy-reporting procedures.

To ensure Network locations meet federally mandated physical security standards, we recommended Deputy Associate Administrator for the Space Communications and Navigation Program and the Network work closely with Headquarters' and Goddard Space Flight Center's Office of Protective Services personnel to:

11. Assess Network locations and ensure logical and physical protection on NASA-owned equipment comply with applicable guidance.

To ensure Network stations remain operational and meet future mission requirements, we recommended the Deputy Associate Administrator for Space Communications and Navigation Program:

12. Direct the Network to perform a thorough assessment of assets and schedule depot-level maintenance.
13. Seek funding to perform depot-level maintenance on the Network's antennas.
14. Work with the Network Project Manager to direct Exelis to identify and track deferred depot-level maintenance as part of its Reliability Plan.

We provided a draft of this report to NASA management, who concurred or partially concurred with our recommendations and described planned corrective actions. With the exception of Recommendation 2, we consider management's comments responsive to our recommendations. Those recommendations are resolved and we will close them upon completion and verification of the proposed corrective actions.

The Associate Administrator for Human Exploration and Operations and the Chief Information Officer partially concurred with Recommendation 2. They agreed to recategorize the portion of the Network that supports the SLS and Orion as a "High" system, but intend to retain the "Moderate" rating for the rest of the Network because it is not critical to the operation of any NASA spacecraft or spacecraft program. We have concerns regarding this rationale. As discussed in our report, we do not believe the Network operates simply as a "pass through" for communications. Rather, Network components must store (albeit temporarily) and process data and commands prior to transmitting to the spacecraft. Given the importance of the Network to the success of NASA Earth science missions and the launch and contingency support it provides other Federal agencies, we continue to believe the entire Network should be categorized as "High." Accordingly, Recommendation 2 is unresolved.

Management's full response to our report is reproduced in Appendix C. Technical comments provided by management have also been incorporated, as appropriate.

---

Major contributors to this report include, Ridge Bowman, Space Operations Director; Loretta Atkinson, Project Manager; Barbara Moody, Team Lead; Jonathan Flugel; Jim Griggs; and Chris Reeves.

If you have questions about this report or wish to comment on the quality or usefulness of this report, contact Laurence Hawkins, Audit Operations and Quality Assurance Director, at 202-358-1543 or [laurence.b.hawkins@nasa.gov](mailto:laurence.b.hawkins@nasa.gov).

Handwritten signature of Paul K. Martin in black ink.

Paul K. Martin  
Inspector General



# APPENDIX A: SCOPE AND METHODOLOGY

We performed this audit from April 2015 through February 2016 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

In May 2013, we announced an audit of the SCan Program and subsequently decided to review each of the Networks separately. In April 2015, we initiated our audit of the Near Earth Network to assess how the Network is (1) managing its IT and physical security risks, (2) addressing its maintenance and operation needs, and (3) effectively using commercial entities to provide communications services to NASA missions.

We utilized the Near Earth Network's System Security Plan to evaluate the IT security posture of the Network at Wallops, Alaska Satellite Facility, and Universal Space Network's North Pole Ground Station Facility. We reviewed the implementation of management, operational, and technical controls on the Network assets. We focused our efforts on key areas of risk management, security awareness, and continuous monitoring. To determine if the Network's IT inventories were accurate, we selected a judgmental sample of Wallops assets and a full inventory check at the Alaska Satellite Facility and physically observed the location of the component and compared its status to the inventories provided. To learn about the Network's application of vulnerability scanning and security configuration management, we requested and reviewed the most recent quarterly scans and held interviews with security management and system administrators. We did not observe active technical controls testing on any Network components due to the Project not owning any security tools.

We evaluated the Near Earth Network's physical security posture by comparing NASA Critical Infrastructure Protection Program requirements for facility security level assessments to the Network's security assignments for its various facilities. We tested the Network's compliance for facility security level protections by interviews, visual observations, and verification during our site visits. We discussed physical security controls and inconsistencies we found with personnel in Wallops' OPS, and with personnel at the Alaska Satellite Facility and Universal Space Network's North Pole Ground Station Facility.

We also reviewed relevant Federal and NASA standards, guidance, and policy documents related to IT and physical security, including:

- FISMA and Homeland Security Act
- Presidential Policy Directives
- FIPS publications
- NIST 800-series special publications (SP)
- Office of Management and Budget and Federal CIO Council guidance
- NPDs, NPRs, and NASA's IT Security Handbooks
- IT security policies and requirements

To evaluate how the Near Earth Network is addressing its maintenance and operation needs, we reviewed several authoritative documents related to maintenance including NPDs and a related Technical Standard, Near Earth Network's Project Plan, the Network's FY 2017 budget submission, contract documentation, and the contractor's risk management working group minutes. We also interviewed SCA's Services Division Director and Operations Manager, Near Earth Network's Ground Stations Manager, and Exelis' Operations Manager and Engineering Technician.

We reviewed Near Earth Network's preventative maintenance schedule listing for ground systems at Wallops, White Sands, and the Alaska Satellite Facility and selected a judgmental sample from each ground station. We traced the sample to supporting documentation to ensure that the planned and scheduled preventative maintenance was performed and that the listings were accurate.

To evaluate how the Near Earth Network is using commercial entities to provide communications services to NASA missions, we analyzed the percentage of tracking passes provided by commercial providers. We reviewed the Track Reports by antenna location for April 2011, April 2012, April 2013, April 2014, and April 2015, a summary of Network Commercial and NASA Tracks for FYs 2005 through 2009, and the Network's summary of NASA and commercial percentages from FYs 2010 through 2021. In addition, we interviewed personnel in the Near Earth Network's Project Office at Goddard, the Alaska Satellite Facility, and the Universal Space Network, in Alaska.

## Use of Computer-Processed Data

We relied on computer-processed data such as budget data, financial management reports, payment records, IT security plan inventories, and reports generated by IT security tools to perform this audit. Generally, we concluded that we could rely upon this data because we were able to assess the data. For example, we reconciled the financial data for Alaska Satellite Facilities May 2014 and May 2015 costs and verified the documentation to official books and records and supporting source documents.

## Review of Internal Controls

We evaluated internal controls, including Federal laws, NIST guidance, and NASA policies and procedures and concluded that the internal controls were generally adequate, except in specific circumstances, as discussed in the body of this report. Our recommendations, if implemented, should correct the weaknesses identified.

## Prior Coverage

During the last 7 years, the NASA Office of Inspector General and the Government Accountability Office (GAO) have issued 8 reports of significant relevance to the subject of this report. Unrestricted reports can be accessed at <https://oig.nasa.gov/audits/reports/FY16> and <http://www.gao.gov>, respectively.

### *NASA Office of Inspector General*

*NASA's Management of the Deep Space Network* (IG-15-013, March 26, 2015)

*Audit of the Space Network's Physical and Information Technology Security Risks* (IG-14-026, July 22, 2014)

*Space Communications and Navigation: NASA's Management of the Space Network* (IG-14-018, April 29, 2014)

*NASA's Information Technology Governance* (IG-13-015, June 5, 2013)

*NASA Faces Significant Challenges in Transitioning to a Continuous Monitoring Approach for Its Information Technology Systems* (IG-12-006, December 5, 2011)

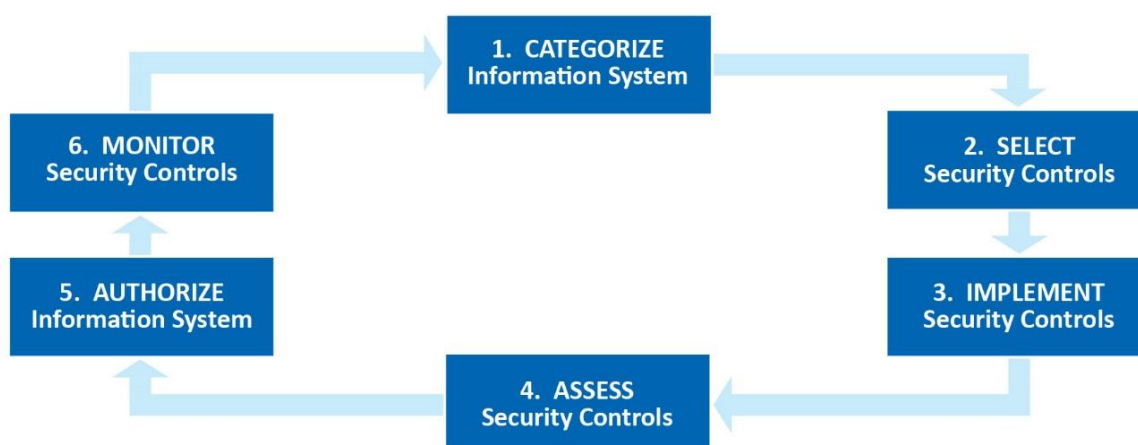
### ***Government Accountability Office***

*Defense Satellite Communications: DOD Needs Additional Information to Improve Procurements* (GAO-15-459, July 17, 2015)

*Satellite Control: Long-Term Planning and Adoption of Commercial Practices Could Improve DoD's Operations* (GAO-13-315, April 18, 2013)

*Information Security: NASA Needs to Remedy Vulnerabilities in Key Networks* (GAO-10-4, October 15, 2009)

# APPENDIX B: NIST RISK MANAGEMENT FRAMEWORK AND ASSOCIATED FEDERAL AND NASA GUIDANCE



## Associated NASA and Federal Guidance Per Life Cycle Step

### 1. CATEGORIZE Information System

- FIPS-199, "Standards for Security Categorization of Federal Information and Information Systems" (2004)
- NIST SP 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems, A Security Life Cycle Approach" (February 2010)
- NIST SP 800-39, "Managing Information Security Risk," Organization, Mission, and Information System View (March 2011)
- NIST SP 800-60 Volumes I and II, "Guide for Mapping Types of Information and Information Systems to Security Categories" (August 2008)
- NPR 2810.1A, "Security of Information Technology" (May 2006)

### 2. SELECT Security Controls

- FIPS-200, "Minimum Security Requirements for Federal Information and Information Systems" (March 2006)
- NIST SP 800-53 Rev 4, "Security and Privacy Controls for Federal Information Systems and Organizations" (April 2013)
- NPR 1600.1A, "NASA Security Program Procedural Requirements" (August 2013)
- NPR 1620.2, "Facility Security Assessments" (October 2012)
- NPR 1620.3, "Physical Security Requirements for NASA Facilities and Property" (October 2012)
- NPR 2810.1A, "Security of Information Technology" (May 2006)
- NASA IT Security Handbooks

### 3. IMPLEMENT Security Controls

- FIPS-200, "Minimum Security Requirements for Federal Information and Information Systems" (March 2006)
- NIST SP 800-70, "National Checklist Program for IT Products – Guidelines for Checklist Users and Developers" (February 2011)
- NPR 1620.3, "Physical Security Requirements for NASA Facilities and Property" (October 2012)
- NASA IT Security Handbooks

### 4. ASSESS Security Controls

- NIST SP 800-53A Rev 4, "Assessing Security and Privacy Controls in Federal Information Systems and Organizations" (December 2014)
- NPR 1620.2, "Facility Security Assessments" (October 2012)
- NPR 1620.3, "Physical Security Requirements for NASA Facilities and Property" (October 2012)
- NPR 2810.1A, "Security of Information Technology" (May 2006)
- NASA ITS-HBK-2810.02-05, "Security Assessment and Authorization: External Information Systems" (October 2012)

### 5. AUTHORIZE Information System

- NIST SP 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems, A Security Life Cycle Approach" (February 2010)
- NASA ITS-HBK 2810.02-2D, "Information System Security Assessment and Authorization Process" (February 2015)
- NASA ITS-HBK-2810.02-05, "Security Assessment and Authorization: External Information Systems" (October 2012)

### 6. MONITOR Security Controls

- NIST SP 800-137, "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations" (September 2011)
- NASA ITS-HBK-2810.02-04A, "Continuous Monitoring – Security Control Ongoing Assessments and Authorization" (March 2014)

# APPENDIX C: MANAGEMENT'S COMMENTS

National Aeronautics and Space Administration  
**Headquarters**  
 Washington, DC 20546-0001



MAR 11 2016

Reply to Attn of:

Human Exploration and Operations Mission Directorate

TO: Assistant Inspector General for Audits

FROM: Associate Administrator for Human Exploration and Operations  
 Chief Information Officer

SUBJECT: Agency Response to OIG Draft Report "Management of the Near Earth Network" (A-15-007-00)

NASA appreciates the opportunity to review and comment on the Office of Inspector General (OIG) draft report entitled "Management of the Near Earth Network" (A-15-007-00), dated February 10, 2016.

In the draft report, the OIG makes 14 recommendations intended to enhance network protection and compliance with Federal and Agency requirements. Some of these recommendations will have cost impacts, some of which may be significant. Once the various studies and actions are complete, NASA can weigh cost vs. risk and make informed decisions on implementation.

Specifically, the OIG recommends the following:

To ensure NASA is properly protecting the Network, the OIG recommends NASA's Office of Protective Services (OPS), the Deputy Associate Administrator for Space Communication and Navigation Program, the Goddard Space Flight Center's (GSFC) Information Technology and Communications Directorate (ITCD) and the GSFC Office of Protective Services personnel:

**Recommendation 1:** Include the Near Earth Network in the NASA Critical Infrastructure Protection Program.

**Management's Response:** Partially Concur. NASA will nominate the Near Earth Network (NEN) as NASA Critical Infrastructure Protection Program (NCIPP). The nomination should identify all network locations where system access occurs and these should be included as network IT access points. This only includes identification of those NASA-owned facilities where network access occurs.

As part of the NCIPP nomination, NASA will conduct a critical evaluation of the NEN's Physical Assets to determine those assets requiring nomination as NASA Critical Infrastructure (NCI). The Agency partial concurrence is limited to supporting the nomination for NCI only for those NASA-owned facility locations where NASA equipment is operated or stored. The Agency does not concur with the nomination for NCI of any physical assets from NEN commercial and partnering facilities where NASA-owned space or equipment is not utilized or stored.

**Estimated Completion Date:** The nomination of the NEN as NCIPP and the identification of those facilities that should be declared NCI will be accomplished by September 30, 2016.

To ensure the Near Earth Network's information technology (IT) security risk management practices comply with Federal and Agency requirements, the OIG recommends NASA's Office of the Chief Information Officer (OCIO), Deputy Associate Administrator for Space Communications and Navigation, GSFC's Information Technology and Communications Directorate, and Network personnel:

**Recommendation 2:** Re-categorize the Network as a High system in line with NIST-recommended impact levels and the Network's criticality to mission operations.

**Management's Response:** Partially Concur. The NEN Launch Communications Stations (LCS) is a critical asset to the Human Spaceflight Program in support of Orion/SLS missions, to provide critical launch data and support commanding of spacecraft during launch operations, and needs to maintain integrity and availability of communications during these events. The LCS will therefore be designated as a High system.

The remainder of the NEN stations will continue to be designated as a Moderate system. With respect to the other NEN space/ground communications elements, no space/ground communications element, nor their interconnecting operational monitoring network, is critical to the continued operation of any NASA spacecraft nor spacecraft program. The NEN has use of many space/ground communications assets, distributed around the world, that can provide alternative services upon the failure of one or more assets. Additionally, each space/ground communication asset can be operated locally, without the need for an interconnecting operational monitoring network. Further, NEN space/ground communications elements do not generate command data nor resolve telemetry data from a spacecraft downlink. All NEN assets operate in a pass-through mode. Therefore, all of the space/ground communications assets available to the NEN, can provide substitute services to supplant the service of one or more failed assets.

The NEN will reevaluate the security classification of its information system, in particular the information types associated with space operations, and the current

security controls of LCS at Ponce de Leon, FL and the Kennedy Uplink Station at the Kennedy Space Center. A reclassification to a High categorization will be addressed with the appropriate tailoring and scoping of the applicable security controls to components of the overall NEN system. The NEN will utilize a phased approach to implementing the various applicable controls throughout the system. The NEN has initiated a study to determine costs, schedule, and risks of implementing the additional stronger security controls. While the final study report hasn't been delivered, the NEN anticipates the restructuring of their security controls implementation to be completed within one year following the receipt of the funds necessary to accomplish the changes.

**Estimated Completion Date:** June 30, 2017.

**Recommendation 3:** Review all Network external systems connections to ensure they are maintained in accordance with National Institute of Standards and Technology (NIST) and NASA guidance and undergo the appropriate level of assessment through the use of NASA's newly developed external systems assessment procedures checklist.

**Management's Response:** Concur. NEN IT Security personnel will follow the guidelines and procedures in NASA IT Security Handbook ITS-HBK- 2810.02-05A Security Assessment and Authorization: External Information Systems to properly assess the IT security postures of the identified external systems to the NEN. The NEN will collaborate with the Goddard IT Security Office and coordinate external assessment activities to determine the best approach for assessing the external systems: a standard assessment and authorization process, or a level of assurance assessment. The NEN will coordinate these activities with external partners and include them as part of a program of continuous monitoring and assessment. These actions are expected to be implemented in the NEN's IT security continuous monitoring and assessment cycle by January 2017.

**Estimated Completion Date:** June 30, 2017 - information system assessed at High consistent with current Continuous Monitoring (ConMon) assessment cycle

To ensure the Network develops a strategy for continuous monitoring including security controls that comply with Federal and Agency requirements, the OIG recommends the GSFC Information Technology and Communications Directorate and Network personnel:

**Recommendation 4:** Provide the Network with NASA-procured vulnerability scanning software and train local Network project personnel on its use in accordance with Agency requirements.

**Management's Response:** Concur. The NEN will utilize the Vulnerability Management tools and sensors offered by the Continuous Diagnostics and

Mitigation (CDM) Program, a Federal IT Security program in which the Department of Homeland Security (DHS) provides Departments and Agencies with IT Security tools to support Information Security Continuous Monitoring (ISCM) and feed the Federal CDM Dashboard. NASA is expected to have these available for implementation by December 2016.

Pending full implementation of the CDM tools/sensors, the NEN and NASA Communications (NASCOM) Mission Network stakeholders will collaborate to develop scan schedules, templates and overall governance. As tools are deployed, all personnel will be trained on use in accordance with Agency requirements.

**Estimated Completion Date:** September 30, 2017

**Recommendation 5:** Implement security baselines to the fullest extent possible on Network systems and access the baselines for changes on a scheduled basis.

**Management's Response:** Concur. The NEN will utilize the Configuration Settings Management (CSM) tools and sensors offered by the CDM Program, a Federal IT Security program in which the DHS provides Departments and Agencies with IT Security tools to support ISCM and feed the Federal CDM Dashboard.

Pending full implementation of the CDM tools/sensors, the NEN and NASCOM Mission Network stakeholders will collaborate to develop security baselines and overall governance. NEN will review NASA baselines as defined by ASCS, document operational deviations and apply settings, as appropriate, in the Network environment.

**Estimated Completion Date:** September 30, 2017

**Recommendation 6:** Develop a process for reporting compliance with security baselines on Network components.

**Management's Response:** Concur. The NEN will utilize the various tools and sensors offered by the CDM Program, a Federal IT Security program in which the DHS provides Departments and Agencies with IT Security tools to support ISCM and feed the Federal CDM Dashboard. The reporting of security compliance will be facilitated by the data aggregation functions of the CDM tools and sensors, and the subsequent reporting of the data through the NASA Risk Information Security Compliance System (RISCS) servers.

**Estimated Completion Date:** December 30, 2017



**Recommendation 7:** Ensure that malware protections are functioning as intended on applicable Network components.

**Management's Response:** Concur. NEN will work with the NASCOM Mission Network to investigate current service offering. If the NEN cannot effectively utilize Agency, NASCOM Mission Network or DHS-provided resources, the NEN will implement malware protections on applicable network components. This will occur within one year of identified and approved funding.

**Estimated Completion Date:** December 30, 2017

**Recommendation 8:** Ensure exemptions requests and IT security waivers are submitted for areas lacking applicable controls.

**Management's Response:** Concur. Agency and Center annual continuous monitoring and assessment processes will be followed to document residual risks and submitted to the appropriate Authorization Officials (AO) for review and acceptance. All waivers and exceptions will be consistent with the in-development Agency process and documented, routed and approved through a NASA RISC workflow.

**Estimated Completion Date:** December 30, 2017

**Recommendation 9:** Develop a strategy that at a minimum includes improved event management and incident response capabilities; monitoring and packet capture capabilities at strategically identified ingress and egress points of the Network locations; and an event auditing and logging strategy on all critical Network components.

**Management's Response:** Concur. The NEN will utilize the Data Aggregation tools and sensors offered by the CDM Program, a Federal IT Security program in which the DHS provides Departments and Agencies with IT Security tools to support ISCM and feed the Federal CDM Dashboard. The NEN will implement a network packet capture capabilities within one year after funding has been identified and approved.

NEN, NASCOM Mission Network and GSFC ITCD stakeholders will work with the NASA Security Operations Center (SOC) to understand the current network security monitoring architecture in place and identify areas where we can bolster monitoring, packet capture and event auditing and logging capabilities.

**Estimated Completion Date:** March 30, 2018

**Recommendation 10:** Integrate NASA Security Operations Center incident reporting into Network discrepancy-reporting procedures.

**Management's Response:** Concur. The NEN will update their Operating Procedures by April 2016 to have potential IT security incidents identified in NEN discrepancy reporting procedures reported to the NASA SOC, accordance with NASA procedures.

**Estimated Completion Date:** April 30, 2016

To ensure Network locations meet federally mandated physical security standards, the OIG recommends the Deputy Associate Administrator for the Space Communications and Navigation Program and the Network work closely with the Headquarters' and GSFC Office of Protective Services personnel to:

**Recommendation 11:** Assess Network locations and ensure logical and physical protection on NASA-owned equipment comply with applicable guidance.

**Management's Response:** Concur. NASA concurs with this recommendation to assess and evaluate NASA-owned facilities and any NEN supporting contractor facilities currently utilizing NASA-owned equipment to ensure logical and physical protection of NASA-owned equipment and compliance with applicable NASA guidance.

**Estimated Completion Date:** The assessments of those assets to ensure logical and physical protection on NASA-owned equipment will be accomplished by March 31, 2017. Implementation requirements for assessment will be submitted to SCaN as part of the PPBE process.

To ensure Network stations remain operational and meet future mission requirements, the OIG recommends the Deputy Associate Administrator for Space Communications and Navigation Program:

**Recommendation 12:** Direct the Network to perform a thorough assessment of assets and schedule depot-level maintenance.

**Management's Response:** Concur. NEN will be submitting its sustaining engineering activities for NASA owned assets, including a thorough assessment of assets and schedule for Depot Level Maintenance (DLM), to SCaN in response to the SCaN Program and Resources Guidelines (PRG) for PPBE 18. This submittal will be presented to SCaN in March 2016. Consistent with the NASA response to Recommendation 13, NEN implementation of Depot Level Maintenance (DLM) across the network will be based on the funds approved and the phasing of the funds received.

**Estimated Completion Date:** April 30, 2016

**Recommendation 13:** Seek funding to perform depot-level maintenance on the Network's antennas.

**Management's Response:** Concur. The NEN will request funding for FY17-FY22 as part of its submission for PPBE18. The NEN implementation of Depot Level Maintenance (DLM) across the network will be based on the funds approved and the phasing of the funds received.

**Estimated Completion Date:** April 30, 2016

**Recommendation 14:** Work with the Network Project Manager to direct Exelis to identify and track deferred depot-level maintenance as part of its Reliability Plan.

**Management's Response:** Concur. The NEN Project Manager will direct Exelis (now Harris) to identify and track deferred DLM as part of its Reliability Plan deliverable in FY17.

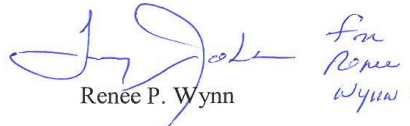
**Estimated Completion Date:** December 30, 2016

We have reviewed the draft report for information that should not be publicly released. As a result of this review, we have not identified any information that should not be publicly released.

Once again, thank you for the opportunity to review and comment on the subject draft report. If you have any questions or require additional information regarding this response, please contact Michelle Bascoe on (202) 358-1574.



William H. Gerstenmaier



Renee P. Wynn

cc:

Director, Goddard Space Flight Center/Mr. Scolese  
 Assistant Administrator, Office of Protective Services/Mr. Mahaley  
 Space Communications and Navigation Program/Mr. Younes  
 Chief Information Officer, GSFC/Mr. VanderTuig  
 Near Earth Network Program Office/Mr. Carter

# APPENDIX D: REPORT DISTRIBUTION

## National Aeronautics and Space Administration

Administrator  
 Deputy Administrator  
 Associate Administrator  
 Chief of Staff  
 Chief Information Officer  
 Associate Administrator, Human Exploration and Operations  
     Deputy Associate Administrator, Space Communications and Navigation Program  
 Assistant Administrator, Office of Protective Services  
 Director, Goddard Space Flight Center  
     Director, Goddard Information Technology and Communications  
 Director, Wallops Flight Facility  
 Project Manager, Near Earth Network

## Non-NASA Organizations and Individuals

Office of Management and Budget  
     Deputy Associate Director, Energy and Space Programs Division  
 Government Accountability Office  
     Director, Office of Acquisition and Sourcing Management  
 National Oceanic and Atmospheric Administration  
     Information Technology Security Program Manager

## Congressional Committees and Subcommittees, Chairman and Ranking Member

Senate Committee on Appropriations  
     Subcommittee on Commerce, Justice, Science, and Related Agencies  
  
 Senate Committee on Commerce, Science, and Transportation  
     Subcommittee on Space, Science, and Competitiveness  
  
 Senate Committee on Homeland Security and Governmental Affairs  
  
 House Committee on Appropriations  
     Subcommittee on Commerce, Justice, Science, and Related Agencies  
  
 House Committee on Oversight and Government Reform  
     Subcommittee on Government Operations  
  
 House Committee on Science, Space, and Technology  
     Subcommittee on Oversight  
     Subcommittee on Space

**(Assignment No. A-15-007-00)**