NASA

National Aeronautics and Space Administration

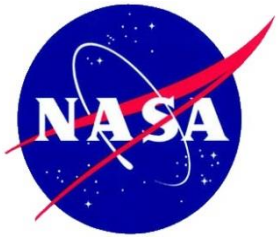
**Office of Inspector General**

**Office of Audits**

# NASA'S MANAGEMENT OF THE DEEP SPACE NETWORK

**March 26, 2015**

**Report No. IG-15-013**




# National Aeronautics and Space Administration

To report, fraud, waste, abuse, or mismanagement, contact the NASA OIG Hotline at 800-424-9183 or 800 535 8134 (TDD) or visit http://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 http://oig.nasa.gov/audits/staff.html.

NASA Office of Inspector General
Office of Audits

# RESULTS IN BRIEF

## NASA's Management of the Deep Space Network

March 26, 2015 IG-15-013 (A-14-012-00)

## WHY WE PERFORMED THIS AUDIT

NASA's Deep Space Network (DSN or Network) is a central component of the Agency's space communications and navigation capability, providing deep space missions with tracking, telemetry, and command services needed to control spacecraft and transmit data. Part of NASA's Space Communications and Navigation (SCaN) Program, DSN operates antennas and transmitters at communications complexes in three locations: Goldstone, California; Madrid, Spain; and Canberra, Australia. NASA has contracts with the Spanish and Australian governments to manage day-to-day operations at the foreign sites and with the Jet Propulsion Laboratory (JPL), a federally funded research and development center in Pasadena, California, for the Goldstone site. During fiscal year (FY) 2014, DSN supported more than 30 missions including the launch and orbit insertions of NASA's Mars Atmosphere and Volatile EvolutioN Mission and the Indian Space Agency's Mars Orbiter Mission.

Much of DSN's hardware is more than 30 years old, costly to maintain, and requires modernization and expansion to ensure continued service for existing and planned missions. Accordingly, in 2009 DSN management proposed an upgrade project to build new antennas and transmitters between 2009 and 2025.

DSN has significant information technology (IT) and physical infrastructure components that it must protect against compromise from cyber attack, espionage, and terrorism. To this end, the JPL, Madrid, and Canberra agreements require each contractor to follow specified Federal and NASA security policies.

We conducted this audit to examine whether DSN is positioned to meet current and future communication commitments and appropriately managing Network IT and physical security risks. We also considered whether NASA is effectively administering the contracts relating to the foreign sites.

## WHAT WE FOUND

Although DSN is meeting its current operational commitments, budget reductions have challenged the Network's ability to maintain these performance levels and threaten its future reliability. Specifically, in FY 2009 the Network implemented a plan to achieve $226.9 million in savings over 10 years and use most of that savings to build new antennas and transmitters. However, in FY 2013 the SCaN Program cut the Network's budget by $101.3 million, causing DSN to delay upgrades, close antennas, and cancel or re-plan tasks. In addition, SCaN officials are considering additional cuts for DSN in FY 2016 that could further delay maintenance and upgrade tasks. Finally, despite these reductions DSN has not revised life-cycle cost estimates for the upgrade project or performed a detailed funding profile beyond FY 2018, making it difficult to effectively plan and justify funding for the project and DSN's future commitments. If budget reductions continue, DSN faces an increased risk that it will be unable to meet future operational commitments or complete the upgrade project on schedule.

We also found that NASA, JPL, and DSN have significantly deviated from Federal and Agency policies, standards, and governance methodologies for the security of the Network's IT and physical infrastructure. For example, the Network's system security categorization process did not consider all DSN mission functions, vulnerability identification and mitigation practices and IT security configuration baseline application did not comply with Federal and Agency policy, and NASA's Security Operations Center is not adequately integrated into JPL's computer network operations. Further, required physical security controls were missing or inconsistently implemented at the three Complexes, procedures to assign security level designations did not comply with NASA policy, required facility security assessments had not been completed, and security waivers or other risk acceptance documentation were not consistently in place. As a result, DSN's IT and physical infrastructure may be unnecessarily vulnerable to compromise.

Finally, NASA has not required the Madrid contractor to provide detailed cost support for contract expenses on a timely basis or ensured the Defense Contract Audit Agency performs incurred cost audits of the Madrid and Canberra contracts on a routine basis. Consequently, NASA cannot ensure approximately $37 million in annual payments made to these contractors is allocable, allowable, and reasonable.

## WHAT WE RECOMMENDED

We made 12 recommendations, including that NASA develop a realistic, accurate, and transparent budget that supports the Network's ability to provide communication services; ensure DSN follows established IT security policies, standards, and governance methodologies; develop a strategy for implementing evolving IT and physical security policies at JPL through means that minimize time-consuming negotiation of formal contract modifications; ensure physical security requirements are implemented consistently across the DSN Complexes; and improve oversight of DSN's foreign contracts.

In response to a draft of our report, management concurred with our recommendations and described planned corrective actions. Because we consider the proposed actions responsive, the recommendations are resolved and we will close them upon verification of the completed actions.

**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

# Acronyms

| | |
|---|---|
| BWG | Beam Waveguide |
| CIO | Chief Information Officer |
| CSIRO | Commonwealth Scientific and Industrial Research Organisation |
| DAEP | DSN Aperture Enhancement Project |
| DCAA | Defense Contract Audit Agency |
| DSN | Deep Space Network |
| FIPS | Federal Information Processing Standards |
| FISMA | Federal Information Security Management Act |
| FSL | Facility Security Level |
| FY | Fiscal Year |
| GAO | Government Accountability Office |
| HEF | High Efficiency |
| INTA | Instituto Nacional de Técnica Aeroespacial |
| ISDEFE | Ingenieria de Sistemas para la Defensa de España S.A. |
| IT | Information Technology |
| JPL | Jet Propulsion Laboratory |
| kW | Kilowatt |
| MAVEN | Mars Atmosphere and Volatile EvolutioN |
| NCI | NASA Critical Infrastructure |
| NIST | National Institute of Standards and Technology |
| NOAA | National Oceanic and Atmospheric Administration |
| NPR | NASA Procedural Requirements |
| OCIO | Office of the Chief Information Officer |
| OIG | Office of Inspector General |
| OPS | Office of Protective Services |
| SCaN | Space Communications and Navigation |
| SOC | Security Operations Center |
| USGCB | United States Government Configuration Baseline |

# INTRODUCTION

Capable of acquiring huge amounts of data and employing rudimentary artificial intelligence to make autonomous decisions, modern spacecraft are significantly more sophisticated than their predecessors. However, even after decades of spaceflight one key requirement has not changed – spacecraft must be able to communicate with Earth to receive commands from human controllers and to return scientific data for study. Accordingly, serious communication failures can render a spacecraft useless and result in the complete loss of a mission.

Given the importance of maintaining communication with spacecraft like the Lunar Reconnaissance Orbiter as it surveys the Moon and Cassini and Voyager as they travel hundreds of millions of miles away from Earth, NASA established the Deep Space Network (DSN or Network) in December 1963. In this audit, we examined whether DSN, part of the Agency's Space Communications and Navigation (SCaN) Program, is positioned to meet its current and future commitments and is appropriately managing information technology (IT) and physical security risks. We also considered whether NASA is effectively administering contracts with the Spanish and Australian government entities that operate two of DSN's three ground stations. This is the second in a series of audits examining the SCaN Program.[1] See Appendix A for details of the audit's scope and methodology.

## Background

DSN provides deep space missions with the tracking, telemetry, and command services required to control and maintain spacecraft and transmit science data. Although DSN primarily services NASA missions, it also supports missions by NASA's international partners. Because of its importance, NASA has designated DSN as NASA Critical Infrastructure (NCI).[2]

To allow for continuous communication with spacecraft traveling through deep space, DSN operates communications complexes in three locations: Goldstone, California; Madrid, Spain; and Canberra, Australia (see Figure 1). NASA pays operating costs for all three sites and has contracts with the Spanish and Australian government entities to manage day-to-day operations for the foreign sites and with the Jet Propulsion Laboratory (JPL), a federally funded research and development center operated pursuant to contract by the California Institute of Technology, for the Goldstone site.

[1] We issued two reports following our first audit: "Space Communications and Navigation: NASA's Management of the Space Network" (IG-14-018, April 29, 2014) and "Audit of the Space Network's Physical and Information Technology Security Risks" (IG-14-26, July 22, 2014).

[2] NCI are operations, functions, physical assets, or IT resources essential to the success of the Agency's mission. NASA considers DSN NCI because of its high public visibility, importance to the accomplishment of NASA missions, high dollar value, and the difficulty of replacing the Network in a reasonable amount of time. Until 2013, the Agency referred to NCI assets as "mission essential infrastructure."

**Figure 1: Locations of Primary DSN Communications Complexes**


Source: NASA Office of Inspector General (OIG) representation of DSN information.

# Organizational Structure of DSN

The DSN Project Office is based at JPL in Pasadena, California. The Project Office is responsible for overall management of all three DSN Complexes and in fiscal year (FY) 2014 executed a $210 million budget covering operations, maintenance, and upgrades to the Network. Also located at JPL, the NASA Management Office is staffed by civil service personnel who oversee the Agency's contract with JPL and administer the contracts with Spain and Australia for the foreign Complexes.

## *Goldstone Deep Space Communications Complex*

The Goldstone Deep Space Communications Complex (Goldstone) is located in the Mojave Desert about 35 miles north of Barstow, California, on the Fort Irwin military base and has been operational since 1958. The Complex is roughly 51 square miles and its remote location is ideal for receiving and transmitting signals from spacecraft. Exelis, Inc., a private contractor specializing in support for space networks, is responsible for on-site management of Goldstone as part of its 5-year, $218.2 million subcontract with JPL. In FY 2014, Exelis had an annual operating budget of $16.8 million for Goldstone and employed about 150 people.

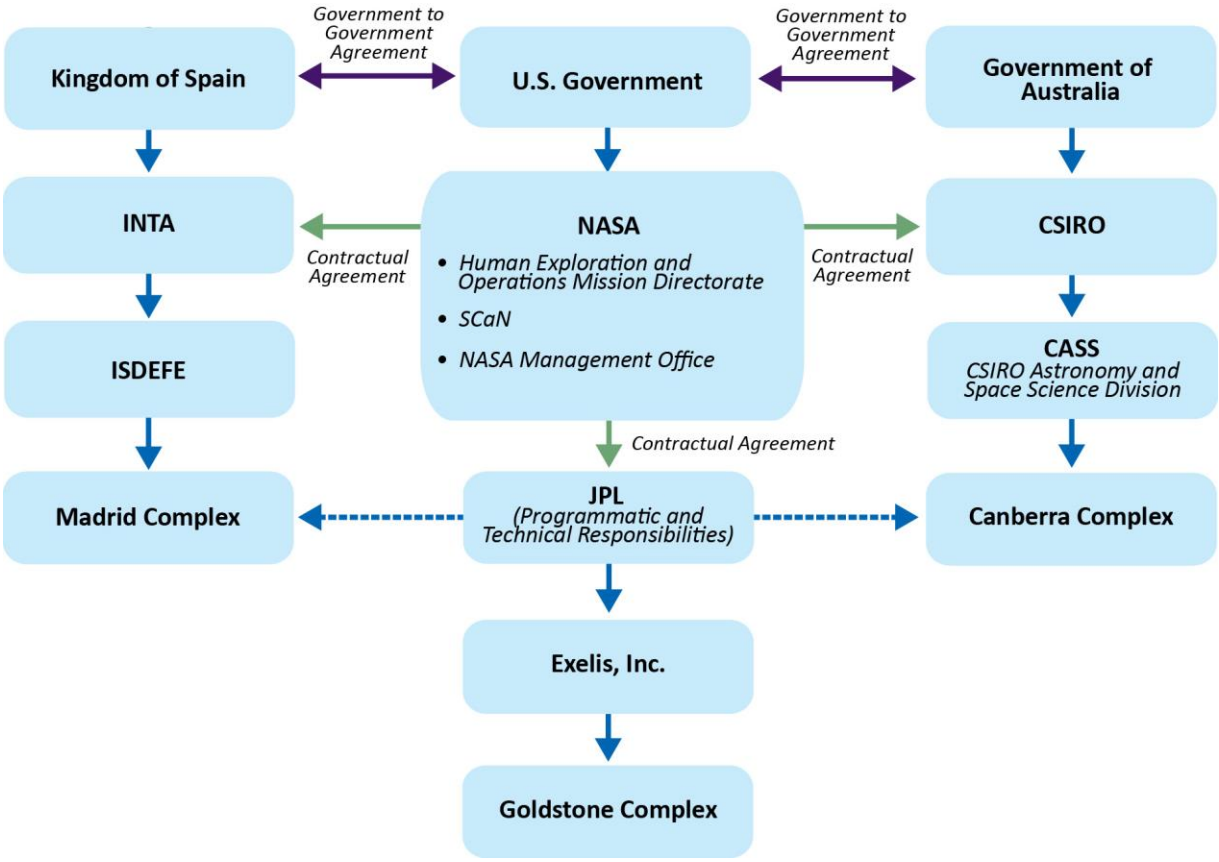
### *Madrid Deep Space Communications Complex*

In accordance with an agreement between the United States and Spain, Ingenieria de Sistemas para la Defensa de España S.A. (ISDEFE), a wholly owned subsidiary of the Instituto Nacional de Técnica Aeroespacial (INTA) and a part of the Spanish Department of Defense, operates and maintains the Madrid Deep Space Communications Complex (Madrid). Located in a mountainous region about 37 miles from the city and operational since 1965, the Complex is roughly 0.30 square miles and employs about 100 people. ISDEFE's operating budget for FY 2014 was $17.6 million.

### *Canberra Deep Space Communications Complex*

The Commonwealth Scientific and Industrial Research Organisation (CSIRO), an Australian Commonwealth Government Statutory Authority, established the CSIRO Astronomy and Space Science Division to manage the day-to-day operations, engineering, and maintenance activities of the Canberra Deep Space Communications Complex (Canberra). Located in a hilly region about 22 miles from Canberra and operational since 1965, the Complex is roughly 0.26 square miles and employs about 100 people. In FY 2014, CSIRO's operating budget for the site was $19 million. See Figure 2 for DSN's organizational structure.

**Figure 2: DSN Organizational Structure**




Source: NASA OIG representation of DSN information.

## DSN Antennas

DSN uses a variety of antennas located at the Complexes and three main spectrum frequency bands – S, X, and Ka – to communicate with spacecraft.[3] The largest antenna at each Complex is a 70-meter parabolic dish antenna. In addition, each Complex has two types of 34-meter antennas: High Efficiency (HEF) and Beam Waveguide (BWG). Specifically, each Complex has one HEF antenna and either three (Goldstone) or two (Madrid and Canberra) BWG antennas. NASA constructed the larger antennas in the mid 1960s and early 1970s as 64-meter antennas, which were later expanded to 70 meters to capture signals from the deepest parts of our solar system.[4] The HEF antennas, built in the mid 1980s, were the first to support higher-frequency transmissions known as X-band uplinks. Built between the mid 1990s and early 2000s, BWG antennas can handle communications in S-, X-, and Ka-band frequencies to support a greater variety of deep space missions.

[3] Sixties-era spacecraft communicated on the S-band. X-band came into use in the 1990s with Ka-band following in the 2000s. Many spacecraft have dual frequency capability (i.e., S/X and more recently X/Ka). The use of higher frequencies for data transmission allows larger bandwidths, which enables faster transmission of larger amounts of data and better tracking capability.

[4] Increasing the diameters of the antennas significantly increased their ability to gather weak microwave signals, particularly from the Voyager 1 and 2 spacecraft launched in 1977, which were hundreds of millions of miles away from Earth exploring the outer planets of the Solar System.

In addition, the BWGs sensitive electronic equipment is stored in an underground room in their pedestals, making the equipment more accessible and enabling easier repair and maintenance compared to the HEFs in which similar equipment is located at the center of the dish. See Figure 3 for a summary of DSN's operational antennas.

**Figure 3: DSN's Operational Antennas as of February 2015**

**70-meter Antenna**

DSS-14: Goldstone, built 1966, expanded 1988
DSS-43: Canberra, built 1973, expanded 1987
DSS-63: Madrid, built 1973, expanded 1987

**34-meter HEF Antenna**

DSS-15: Goldstone, built 1984
DSS-45: Canberra, built 1986
DSS-65: Madrid, built 1987

**34-meter BWG Antenna**

DSS-24: Goldstone, built 1994
DSS-25: Goldstone, built 1996
DSS-26: Goldstone, built 1996
DSS-34: Canberra, built 1997
DSS-35: Canberra, built 2014
DSS-54: Madrid, built 1998
DSS-55: Madrid, built 2003

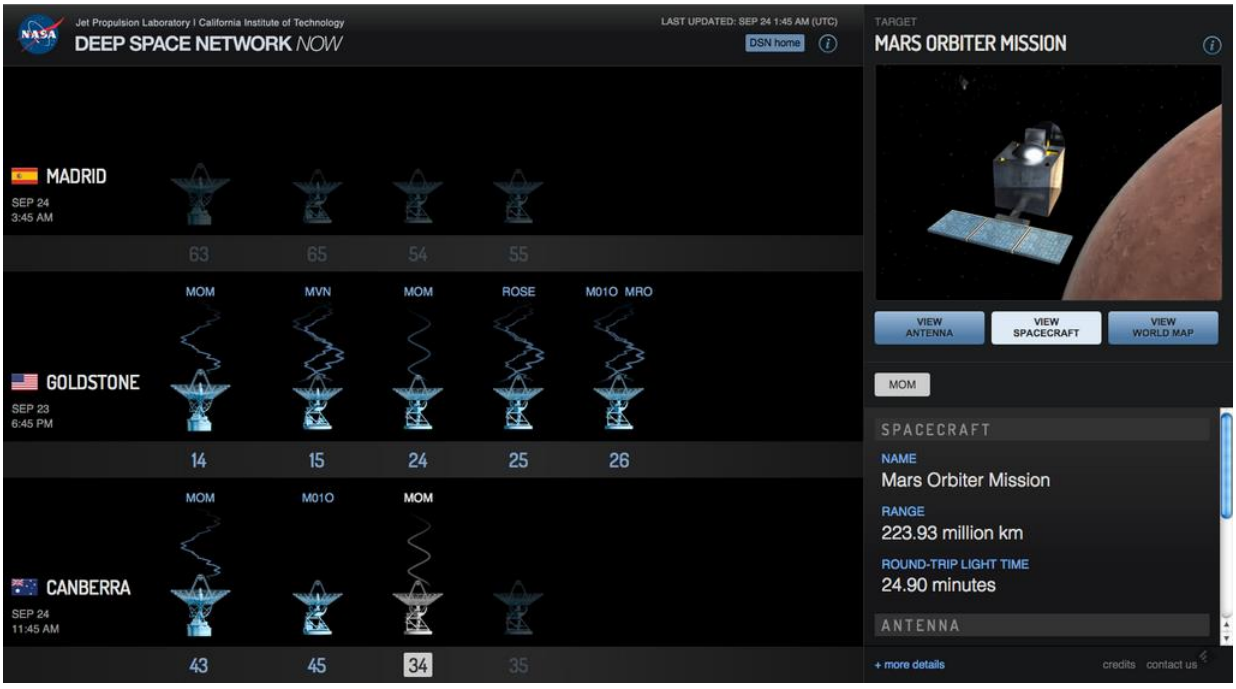
Source: NASA OIG representation of DSN information.

Because of the significant distance they must travel, communication signals between spacecraft traveling in deep space and Earth is extremely challenging. Adding to the complexity is that the communication equipment on such spacecraft tends to be small and lightweight and transmits at very low power (as low as 20 watts). Consequently, the power of signals arriving at DSN antennas can be as weak as a billionth of a billionth of a watt or 20 billion times weaker than the power required to run a digital wristwatch. Moreover, the demands placed on NASA's deep space communications system are increasing. For example, as of 2013 the Mars Reconnaissance Orbiter had sent back to Earth nearly 25 terabytes of data.[5] Even at its top data transmission rate of 5.2 megabits per second, the Orbiter requires 7.5 hours to empty its onboard recorder and 1.5 hours to send a single high-resolution image back to Earth for processing.

[5] Mars Reconnaissance Orbiter, launched in August 2005, entered Martian orbit in March 2006 to map the planet's landscape and study its climate, atmosphere, and geology.

During FY 2014, the Network supported more than 30 missions including the launch and orbit insertions of NASA's Mars Atmosphere and Volatile EvolutioN (MAVEN) Mission and the Indian Space Agency's Mars Orbiter Mission (see Figure 4). DSN also supports the Mars Curiosity Rover as it travels on the surface of Mars and the European Space Agency's Rosetta Mission, which in November 2014 landed scientific instruments on a comet traversing between Mars and Jupiter. Missions planned for FY 2015 include a flyby of Pluto by NASA's New Horizons spacecraft.[6] Beyond FY 2015, NASA is planning for the launch of the James Webb Space Telescope and the Solar Probe Plus, missions that will place additional demands on DSN.

**Figure 4: Snapshot of DSN Antennas' Communication Activity during Mars Orbiter Mission's Mars Orbit Insertion**




Source: NASA, "Deep Space Network Now," http://eyes.nasa.gov/dsn/dsn.html (last accessed on September 23, 2014).

Note: MVN refers to the MAVEN Mission; ROSE refers to European Space Agency's Rosetta Mission; M01O refers to Mars Odyssey spacecraft; and MRO refers to the Mars Reconnaissance Orbiter, all of which were transmitting or receiving data from DSN at the time of insertion.

# Operation of DSN

DSN operates continuously to ensure uninterrupted communications coverage. NASA missions supported by DSN do not pay for use of the Network unless a unique technology must be added to provide coverage. During a mission's development, Network officials meet with the mission team to determine the type and amount of communications coverage the mission will need, including the amount of time per day for routine communications and coverage for such major events as insertion into planetary orbit. In most cases, missions request more coverage than DSN is capable of providing,

[6] New Horizons, launched in January 2006, is the first scientific investigation to obtain a close look at Pluto and its moons Charon, Nix, Hydra, Kerberos, and Styx. The spacecraft is expected to reach Pluto in July 2015, where it will transmit data about the dwarf planet and its moons' surface properties, geology, interior makeup, and atmosphere.

and therefore must negotiate with the Network and other DSN customers for additional coverage when possible. Once the amount of communications coverage is established and major mission events are scheduled, DSN commits to providing coverage in a service agreement with mission personnel.

DSN promises 95 percent availability to its customers for routine mission coverage, with 5 percent reserved for unexpected failures and downtime. Since FY 2009, DSN has operated at more than 98 percent proficiency in providing coverage to its customers.[7] However, DSN officials warn it will be increasingly difficult to maintain this level of service with an aging infrastructure and note they have been deferring long-term maintenance projects to fit budget constraints.

## Future Operations of DSN

Historically, all three DSN Complexes have operated continuously, with three shifts per day and one operator per antenna. For example, if three antennas were in operation at each of the Complexes, nine operators – three at each Complex – would be on duty at any one time. In FY 2009, DSN estimated that it could save almost $31 million through FY 2018 by implementing a "follow-the-Sun" concept pursuant to which all antennas would be operated from one Complex and each operator at that Complex would be responsible for three antennas. So, for example, making the same assumption of three operating antennas at each Complex, during daylight hours in California three operators at Goldstone would operate all nine antennas. Subsequently, during daylight hours in Spain, three operators in Madrid would take over, followed by three operators at Canberra. The remaining two shifts at each Complex would consist of a small staff to respond to emergencies. The Network implemented the first phase of "follow-the-Sun" operation in FY 2014 by transitioning from one to two antennas per operator. It hopes to achieve full "follow-the-Sun" operation by 2018 and plans to invest the resulting savings toward upgrading and expanding DSN's antenna architecture.

## DSN Aperture Enhancement Project

Because much of its hardware is over 30 years old and difficult and costly to maintain, DSN requires modernization and expansion to ensure continued service for existing and planned missions. In 2009, DSN proposed an upgrade program – the DSN Aperture Enhancement Project (DAEP) – to build new antennas and transmitters.[8] DSN proposed that by the end of FY 2025, DAEP will provide six new 34-meter BWG antennas, each equipped with a 20 kilowatt (kW) transmitter, and six new 80 kW high power transmitters (two at each Complex) at a total cost of $362.4 million. With the new antennas, DSN will be able to array 34-meter BWG antennas so they supply downlink capabilities similar to a 70-meter antenna. Similarly, installation of an 80 kW transmitter in the 34-meter antennas will provide uplink capability comparable to the 70-meter antennas. DSN proposed to construct the new antennas and transmitters in phases.

[7] Proficiency is calculated by the actual service time provided divided by the service time scheduled.

[8] DSN proposed to fund these upgrades through savings from implementing concepts like "follow-the-Sun" and reducing operations and maintenance costs.

### *Phase 1*

Because the needs of spacecraft traveling in the Southern Hemisphere will begin to overload existing X- and Ka-band capacity at Canberra by 2015, DSN planned to construct the first two new BWG antennas there. In addition, DSN is designing, developing, and deploying three 80 kW X-band uplink systems (one at each Complex) and developing new 20 kW transmitters for the new Canberra antennas. The first Canberra antenna (DSS-35) became operational in October 2014. DSN anticipates the second antenna (DSS-36) will be operational in FY 2016. Although the 80 kW transmitter for Goldstone is on schedule for FY 2015 operations, the Canberra and Madrid transmitters are not expected to be operational until FYs 2020 and 2021, respectively.

### *Subsequent Phases*

Over the next 10 years, DAEP will install two new BWG antennas in Madrid, an additional BWG antenna at Canberra, and a BWG antenna at Goldstone. In addition, plans are in place to install a second 80 kW transmitter at each Complex. Originally, the Network planned to complete construction of the third antenna at Canberra before starting work at the other Complexes; however, the pedestals of two existing antennas at Madrid (the 70-meter antenna and a 34-meter antenna) are showing considerable concrete degradation that must be resolved. As a result, DSN delayed the third Canberra antenna and accelerated the construction schedule for the Madrid antennas as a contingency against future long-term maintenance downtime. Upon completion of the Madrid antennas and the third Canberra antenna, DSN plans to deploy the final antenna at Goldstone.

## IT and Physical Security Controls for the DSN

With both IT and physical infrastructure components, DSN must protect against various kinds of threats, including cyber attacks, espionage, adversarial nation states, and terrorist organizations. Indeed, in 2009 and 2011 hackers from the Netherlands and China compromised multiple DSN support components through separate attacks. NASA's Office of the Chief Information Officer (OCIO) is responsible for the security of NASA's IT assets and NASA's Office of Protective Services (OPS) for the security of its personnel, operations, property, and physical infrastructure. JPL's Chief Information Officer (CIO) and OPS are responsible for ensuring applicable Agency policies are implemented at the DSN Complexes.

### *Contractual Requirements for the Security of DSN*

The JPL, Madrid, and Canberra contracts require each contractor to follow specified Federal and NASA security and privacy policies and regulations. The contractors are also required to support NASA in meeting the legal and policy mandates associated with managing U.S. Government IT infrastructure, systems, assets, and information.[9] JPL's contract also includes the requirement to follow tailored NASA policy governing physical security assessments and requirements.[10] Although the Madrid and Canberra contracts do not reference specific NASA physical security policies, the contract and supplemental task description both describe the Complexes as "minimum essential infrastructure that NASA considers necessary for accomplishing its mission" and require physical security measures be implemented jointly with NASA.

[9] NASA Federal Acquisition Regulation Supplement 1852.204-76, "Security Requirements for Unclassified Information Technology Resources."

[10] JPL NASA Procedural Requirements (NPR) 1620.2 "Facility Security Assessments," October 14, 2011, and JPL NPR 1620.3A, "Physical Security Requirements for NASA Facilities and Property," October 14, 2011.

### *Legislative Authority and Guidance for IT and Physical Security*

The Federal Information Security Management Act (FISMA) of 2002 and the Homeland Security Act of 2002 provide guidance to agencies in securing Federal information systems, data, and physical infrastructure.[11] FISMA requires Federal agencies to develop, document, and implement an agency-wide program to provide security for the information and related systems that support their operations and assets. The Homeland Security Act established the U.S. Department of Homeland Security, which developed physical security standards for Federal agencies, facilities, and infrastructure.

To help implement FISMA, the National Institute of Standards and Technology (NIST) developed standards and special publications that provide agencies with a standard risk management framework.[12] Using NIST risk management tools and techniques is essential to developing, implementing, and maintaining safeguards and countermeasures to mitigate threats. 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.

NASA adopted NIST standards and Homeland Security Act measures, and the OCIO and OPS work together to ensure alignment of security objectives and develop Agency policies and guidelines. Further, the OCIO and OPS have partnered to form the NASA Critical Infrastructure Protection Program through which they identify, plan, and implement enhanced security measures for NCI. OPS has responsibility for conducting assessments for the Protection Program and collaborates with the OCIO and Center CIOs to ensure critical cyber assets are identified and included in the Agency's NCI inventory.

As part of the Protection Program, NASA developed policies addressing physical security for NCI facilities and property.[13] These policies assist NASA organizations in identifying and prioritizing protections for their assets and require them to designate facilities as one of four Facility Security Levels (FSL). NASA policy requires NCI facilities to carry at least a FSL III designation and organizations to consider all available funding sources to implement security-related efforts.

[11] FISMA is Title III of the E-Government Act of 2002. See: E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899 (2002). For the Homeland Security Act, see: Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (2002).

[12] Federal Information Processing Standards (FIPS) publications and the supporting NIST 800-series of special publications.

[13] NPR 1600.1A, "NASA Security Program Procedural Requirements," August 12, 2013; NPR 1620.2A, "Facility Security Assessments," October 4, 2012; and NPR 1620.3A, "Physical Security Requirements for NASA Facilities and Property," October 4, 2012.

# BUDGET REDUCTIONS AND UNCERTAINTY OF PROJECTED FUTURE SAVINGS INCREASE RISK TO NASA'S PLAN TO BUILD NEW ANTENNAS AND TRANSMITTERS

Although DSN is currently meeting its operational commitments, budget reductions have challenged the Network's ability to maintain these performance levels and threaten future reliability. In FY 2009, the Network implemented a plan to achieve $226.9 million in savings over 10 years and directed $217.6 million to building new antennas and transmitters. However, in FY 2013 SCaN reduced the Network's budget by $101.3 million, causing DSN to delay DAEP, close antennas, and cancel or re-plan tasks. In addition, SCaN officials are considering additional reductions for DSN in FY 2016 that, according to Project officials, would further delay maintenance and upgrade tasks. Finally, despite these reductions DSN has not updated DAEP's life-cycle costs or performed a detailed funding profile beyond FY 2018, making it difficult to effectively plan for and justify funding for DAEP and DSN's future commitments.

## DAEP is Adequately Funded through FY 2015

In FY 2009, DSN proposed that by 2025 it could achieve sufficient savings from efficiency measures to invest in six new 34-meter antennas (three at Canberra, two at Madrid, and one at Goldstone), six new 80 kW transmitters (two at each Complex), and six new 20 kW transmitters (one on each new 34-meter antenna). The savings would come from implementing "follow-the-Sun" ($30.9 million) and reducing DSN operations ($68.5 million), 70-meter antenna uplink costs, Exelis' subcontract costs, and reserves ($78.1 million). The remaining proposed savings ($49.4 million) would come from delaying and re-planning antenna- and facilities-related tasks such as power modernization, surveillance systems, and Goldstone's roofing and water system. The efficiency measures have thus far been sufficient to fund DAEP upgrades through FY 2015.

## Budget Reductions Pressed DSN to Find Additional Savings, Resulting in Increased Costs

In March 2013, 4 years after DSN began implementing its plan to use savings to fund DAEP, SCaN directed the Network to reduce its overall budget by $101.3 million for FYs 2013 through 2019. These cuts were primarily due to sequestration, other SCaN priorities, and an Agency directed 1 percent reduction for all programs (see Table 1).

**Table 1: Proposed DSN Budget Reductions**

| Description (dollars in millions) | Fiscal Year | | | | | | | Total |
|---|---|---|---|---|---|---|---|---|
| | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 | |
| Sequestration | $8.94 | $9.05 | $9.50 | $9.56 | $9.17 | $9.93 | $9.89 | **$66.04** |
| Other SCaN Priorities | | 10.00 | 10.00 | | | | | **$20.00** |
| Agency 1 Percent Reduction | | | 2.00 | 1.55 | 1.86 | 1.92 | 1.92 | **$9.25** |
| Other[a] | | 5.50 | (2.00) | 2.34 | 0.07 | (2.93) | 3.00 | **$5.98** |
| **Total** | **$8.94** | **$24.55** | **$19.50** | **$13.45** | **$11.10** | **$8.92** | **$14.81** | **$101.27** |

Source: NASA OIG representation of DSN information.

[a] Other represents about 6 percent of the total cuts and includes $9 million in FY 2015 for partial restoration of other SCaN priorities, the Agency's 1 percent reduction, and adjustments of $18.6 million for inflation factors for FYs 2016 through 2018.

By absorbing $8.94 million in cuts for FY 2013 and proposing actions to offset $91.7 million between FYs 2014 and 2019, the Network developed a plan that would address all but $600,000 of the $101.3 million budget reduction. Specifically, DSN proposed to delay key components of DAEP; negotiate with Exelis to achieve cost savings in the Goldstone contract; reduce personnel at JPL, Madrid, and Canberra; close antennas; and cancel and delay maintenance facility tasks. However, some of these actions have the effect of increasing overall costs for the Network and pose a risk DSN will not achieve the savings the Network has targeted to fund DAEP. For example, DSN plans to reduce expenses by approximately $10 million in FYs 2014 and 2015 by delaying installation of Canberra's third antenna and the 80 kW transmitters at Madrid and Canberra. However, this means to keep DAEP on schedule for completion by 2025, the Network will incur an additional $18.6 million in inflation costs in FYs 2016 through 2018. Further, during development of the plan it became clear that certain maintenance and operations tasks, such as addressing concrete degradation of the Madrid antennas, would have to be addressed, which reduced planned savings. Table 2 provides a summary of DSN's plan to offset the budget reductions.

**Table 2: DSN's Planned Actions to Offset Budget Reductions**

| Item/Description (dollars in millions) | Fiscal Year | | | | | | Total |
|---|---|---|---|---|---|---|---|
| | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 | |
| Antenna/Transmitter Delay | $5.00 | $5.00 | $(3.15) | $(6.25) | $(9.25) | N/A | **$(8.65)** |
| New Goldstone Contract | 9.87 | 10.84 | 12.30 | 14.30 | 15.77 | 15.77 | **78.85** |
| Reductions | 3.66 | 4.57 | 5.55 | 5.72 | 6.50 | 6.50 | **32.50** |
| Antenna Closures[a] | 2.28 | 4.50 | 7.40 | 0.96 | 1.29 | 0.95 | **17.38** |
| Additional Funding | 4.35 | N/A | N/A | N/A | N/A | N/A | **4.35** |
| Cancelled and Delayed Tasks | 1.85 | 0.35 | 1.46 | 3.21 | 2.48 | (3.50) | **5.85** |
| Long-Term Maintenance and Operations Costs | (2.51) | (5.93) | (10.08) | (6.95) | (8.28) | (4.81) | **(38.56)** |
| **Total Savings** | **$24.50** | **$19.33** | **$13.48** | **$10.99** | **$ 8.51** | **$14.91** | **$91.72** |

Source: DSN Budget Challenge and Response.

[a] Of the $17.38 million in antenna closures, $16.36 million is associated with the proposed closure of the HEF antennas. The remaining $1.02 million is savings from decommissioning Goldstone's 34-meter high-speed BWG antenna in December 2013.

## Planned Actions to Offset Budget Reductions Resulted in DAEP Schedule Delays and Operational Risks

Because of the budget reductions described above, key components of DAEP have been delayed and work has been reshuffled. For example, DSN planned to build the first three of six new 34-meter antennas at Canberra (operational by 2018) before building two more at Madrid (operational in FY 2020 and 2022, respectively).[14] Although DSN still expects to complete the two Canberra antennas and one 80 kW transmitter at Goldstone on time, the budget reductions forced a delay of the third planned antenna by 1 year and delayed all four 80 kW transmitters planned for Canberra and Madrid by as much as 4 years. Additionally, a recently identified structural issue in one of the existing 34-meter antennas at Madrid caused DSN to move the third antenna build from Canberra to Madrid. DSN will also build the fourth antenna in Madrid thereby enabling the site to receive its new antennas 2 years earlier than originally planned and delaying Canberra's third antenna (now the fifth antenna build) until 2022.[15] (See Table 3.)

[14] The sixth and final antenna is planned for Goldstone.

[15] DSN is also evaluating the placement of the third Canberra antenna in an alternate location in Africa or South America to provide backup capability to Canberra in the Southern Hemisphere.

**Table 3: Schedule for DAEP Antenna and Transmitter Upgrades**

| Description/Location | Original Operational Dates | Current Operational Date | Delay |
|---|---|---|---|
| Antenna DSS-35/Canberra | FY 2014 | FY 2014 | None |
| Antenna DSS-36/Canberra | FY 2016 | FY 2016 | None |
| Antenna DSS-33/Canberra | FY 2018 | FY 2022 | 4 Years |
| Antenna DSS-56/Madrid | FY 2020 | FY 2019 | None[a] |
| Antenna DSS-53/Madrid | FY 2022 | FY 2020 | None[b] |
| Antenna DSS-23/Goldstone | FY 2024 | FY 2024 | None |
| 80 kW Transmitter DSS-26/Goldstone | FY 2015 | FY 2015 | None |
| 80 kW Transmitter DSS-35/Canberra | FY 2016 | FY 2020 | 4 Years |
| 80 kW Transmitter DSS-55/Madrid | FY 2017 | FY 2021 | 4 Years |
| 80 kW Transmitter DSS-36/Canberra | FY 2018 | FY 2022 | 4 Years |
| 80 kW Transmitter DSS-56/Madrid | FY 2020 | FY 2023 | 3 Years |
| 80 kW Transmitter DSS-23/Goldstone | FY 2024 | FY 2024 | None |

Source: NASA OIG representation of DSN information.

[a] DSS-56 is 1 year ahead of plan.
[b] DSS-53 is 2 years ahead of plan.

In addition to delaying key components, budget reductions will require DSN to accept additional operational risks. Specifically, the plan includes decommissioning the 34-meter HEF antennas currently operating at each Complex between FYs 2016 and 2018 and shifting the work to the BWG antennas to generate a proposed savings of $16.4 million. However, closing these antennas increases the risk the Network will not be able to support future operational needs. Specifically, during FY 2014 DSN utilized about 72.9 percent of the HEF antennas' available tracking hours, and DSN's own data shows that for FYs 2016 through 2019 its current 34-meter antennas, including the HEF antennas, are oversubscribed by an average of 20.7 percent. When the HEF antennas are decommissioned, the average unsupportable requested antenna time could be as high as 25.5 percent (an increase of 4.8 percent), which could limit DSN's ability to transmit scientific data for missions such as the Solar and Heliospheric Observatory.[16]

Moreover, unlike the HEF antennas, some of the BWGs required to replace the HEF antennas do not have S-band capability. Therefore, DSN plans to upgrade the BWG antennas at a cost of $2.7 million to provide this capability before decommissioning the HEF antennas. Any delay in completing the upgrade would require DSN to push out the planned decommissioning dates, which, in turn, would affect the estimate of planned savings. Finally, because the decommissioning is slated to occur before completion of the two new antennas planned for Madrid, those antennas will not be available to pick up any excess requests for antenna time.

[16] The unsupportable percentage is the amount of requested antenna hours that cannot be provided. The Solar and Heliospheric Observatory Mission, launched in 1995, is an international collaboration between the European Space Agency and NASA to study the Sun from its deep core to outer corona and the solar wind.

## Additional Budget Reductions Would Increase Consequences to DSN

In addition to the reductions discussed above, SCaN officials are considering additional cuts to DAEP. Specifically, in preparing for the FY 2016 budget request, SCaN directed DSN to estimate the impact of eliminating funding to account for inflation in budget estimates for FYs 2016 through 2018. DSN estimated a total of $18.6 million in inflation costs for those 3 years, and concluded that removing that money from the budget would force a delay of 11 tasks, 6 of which have the highest risk rating (high consequence of occurrence and very high impact), and 5 have the second highest rating (moderate consequence and high impact). These tasks include replacing the elevation bearings on the 70-meter antennas at the three Complexes, fixing cracks in Madrid's 70-meter antenna's pedestal, and addressing concrete degradation on a Madrid 34-meter antenna pedestal. Delaying these tasks increases the risk the antennas will fail or need to be taken out of service for maintenance for an extended period. In addition, although DSN did not estimate any cost increases associated with delaying these tasks, the costs of completing them are likely to be higher in later years due to inflation.

# Revised Life-Cycle Cost Estimate and Updated Efficiency Savings for DAEP Would Better Ensure Adequate Funding for DSN

In our judgment, DSN's cost and schedule estimates for DAEP are incomplete. Not only have budget reductions and the potential loss of funding to cover inflation delayed and added significant risk to funding DAEP through FY 2018, NASA has not addressed potential cost increases or schedule delays beyond 2018. Moreover, since March 2010 DSN has not included a full life-cycle cost estimate or funding profile through FY 2025 in its budget submissions. In addition, DSN's calculations of the budget savings it intends to dedicate to DAEP have not been updated for FYs 2019 through 2025. Given these factors and that DSN's budget challenges change each year, it will be difficult for the Agency to effectively determine, plan for, and justify DAEP's future funding needs.

DAEP is not required to follow NASA's policies on life-cycle cost review requirements – requirements that recommend managers develop life-cycle cost estimates for their projects and update the estimate as the project transitions from one phase of the life cycle to the next.[17] Such a review provides a periodic assessment of the technical and programmatic health of the project, including the funding that will be committed during each year, and is designed to prevent development delays in future years caused by inadequate funding levels.[18] The Government Accountability Office (GAO) has noted the importance of life-cycle cost estimates as a best practice to account for program uncertainties, forecast a minimum and maximum range for all life-cycle costs, and clearly define the characteristics of each increment of capability.[19]

[17] Life-cycle cost estimate reviews are not required because DAEP is considered a non-flight project with no defined end, is managed and funded internally by DSN, and will consist of incremental fixed-price JPL subcontracts.

[18] NPR 7120.5E, "NASA Space Flight Program and Project Management Requirements w/Changes 1-10," August 14, 2012.

[19] GAO, "NASA: Actions Needed to Improve Transparency and Assess Long-Term Affordability of Human Exploration Programs" (GAO-14-385, May 8, 2014).

We requested the Network give us an updated life-cycle cost estimate through FY 2025. In response, DSN provided an estimate of $393.1 million – $30.7 million more than its last estimate completed in 2009. Moreover, although DAEP completed a lessons learned study in April 2014, the Network did not determine or incorporate in its projections any cost savings associated with implementing the practices identified.

NASA needs greater assurance that DAEP will be implemented in a manner that ensures the operational needs of the Agency and other missions will be met within budget and cost constraints. Budget reductions have already forced DSN to delay and remove operations and sustainment tasks to ensure continued funding for DAEP. If the reductions continue, the Network faces an increased risk it will be unable to complete DAEP on schedule and meet its future operational commitments. Comprehensive cost estimates for DAEP are a key part of determining, planning, and justifying the budgets necessary to meet these operational commitments.

# DSN Not in Compliance with NASA and Federal IT Security Policies

We found JPL has significantly deviated from established IT security policies, standards, and governance methodologies in attempting to ensure applicable safeguards are implemented at DSN. Specifically, JPL's system security categorization process did not consider all DSN mission functions, its IT security database inventory was inaccurate, vulnerability identification and mitigation practices were not in accordance with Agency policy, security configuration baseline application did not comply with Federal and Agency policy, and NASA's Security Operations Center (SOC) was not adequately integrated into JPL's computer network operations. These issues persist due to weaknesses in contract development and contractor oversight. As a result, NASA does not have adequate safeguards in place for protecting DSN systems, leaving the Network more susceptible to compromise. DSN's upcoming authorization cycle provides JPL with an opportunity to meet evolving Agency and Federal guidelines and improve its IT security program.

## System Security Categorization Did Not Reflect All DSN Missions

JPL rated DSN's security impact as "Moderate." In reaching this conclusion, JPL IT security personnel characterized the system as not including two NIST information types: "Space Operations" and "Disaster Monitoring and Prediction."[20] Including these information types would have raised DSN's impact level to "High" and triggered additional security measures to better protect the confidentiality, integrity, and availability of the information processed through the system.[21] Given the importance of DSN to the success of many NASA missions, we believe a higher security rating for the system would be appropriate.

### NIST Categorization Process

The first step in NIST's Risk Management Framework is categorizing the system based on the information it processes, stores, and transmits. NIST's security categories are based on the potential impact to an organization should certain adverse events occur that would jeopardize the information and information systems the organization needs to accomplish its mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Information systems are categorized as "High," "Moderate," or "Low" after considering all of the information types they process

[20] According to NIST, the "Space Operations" category applies to the safe launch or missions of passengers or goods into aerospace and includes commercial, scientific, and military operations. "Disaster Monitoring and Prediction" involves actions taken to predict when and where a disaster may take place and communicate that information to affected parties. NIST recommends a "High" security impact for systems containing either type of information.

[21] Confidentiality preserves the authorized restrictions on information access and disclosure, including the means for protecting personal privacy and proprietary information. Integrity guards against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. Availability ensures the timely and reliable access to and the use of information.

and based on the final risk determination. NIST publications provide guidelines recommending the types of information and information systems to be included in each category, the minimum-security requirements for each category, and the recommended controls.[22] Among the many information types identified by NIST are "Space Operations" and "Disaster Monitoring and Prediction."

## JPL's Categorization Process

JPL IT security personnel used internal guidance to categorize the DSN system. As shown in Figure 5, JPL traced its security categorization back to the equivalent of three NIST information types: "Space Exploration and Innovation," "IT Infrastructure Maintenance," and "Record Retention," resulting in a Moderate rating for the system.[23]

**Figure 5: JPL Security Categorization Determination Matrix for DSN**

| FIPS PUB 199 | NIST 800-60 Recommended Security Categorization | | | | | JPL Security Categorization | | | |
|---|---|---|---|---|---|---|---|---|---|
| FIPS 199 High Water Mark | Mission/ Management Areas * | Information Types | Confidentiality | Integrity | Availability | Associated JPL Information Categories | Confidentiality | Integrity | Availability |
| Moderate | *General Science and Innovation* | Space Exploration and Innovation | Low | Moderate | Low | Mission (MSN) Information Category | Low | Moderate | Moderate |
| Moderate | *General Science and Innovation* | Space Exploration and Innovation | Low | Moderate | Low | Business and Restricted Technology (BRT) Information Category | Moderate | Moderate | Low |
| Low | *Information & Technology Management* | IT Infrastructure Maintenance | Low | Low | Low | Scientific, Engineering, and Research (SER) Information Category | Low | Low | Low |
| Low | *Information & Technology Management* | Record Retention | Low | Low | Low | Administrative (ADM) Information Category | Low | Low | Low |
| | * 800-60 includes Information Types from Federal Mission Areas or Service Delivery Mechanisms, and from Management and Support Lines of Business | | | | | JPL Tailoring: MSN Availability raised to Moderate to better protect mission operations activities; BRT Confidentiality raised to Moderate to better protect business and restricted technology (e.g., export controlled and privacy information) | | | |

Source: Flight Network System Security Plan 11.

[22] FIPS Publication 199, "Standards for Security Categorization of Federal Information and Information Systems," February 2004; FIPS Publication 200, "Minimum Security Requirements for Federal Information and Information Systems," March 2006; and NIST Special Publication 800-60 Volume I, "Guide for Mapping Types of Information and Information Systems to Security Categories," August 2008.

[23] "Space Exploration and Innovation" includes all activities devoted to innovations directed at human and robotic space flight and the development and operation of space launch and transportation systems, and the general research and exploration of outer space. "IT Infrastructure Maintenance" involves the planning, design, implementation, and maintenance of an IT infrastructure to effectively support automated needs (i.e., operating systems, applications software, platforms, networks, servers, and printers) and includes information systems configuration and security policy enforcement information. "Record Retention" involves operations surrounding management of an agency's official documents and records.

### *Space Operations*

JPL IT security personnel told us they did not include "Space Operations" in their system categorization because, in their assessment, the information type pertains exclusively to the U.S. Department of Transportation and addresses transportation of "passengers or goods." In their view, DSN supports robotic space flight and transmission of scientific data rather than transportation of passengers or goods. However, we note that NIST Special Publication 800-60 Volume II, Section D.11, states that "Transportation" involves "all federally supported activities related to the safe passage, conveyance, or transportation of goods and/or people."[24] Moreover, we spoke with NIST officials who confirmed that NIST information types are specific to systems and not limited to individual departments or agencies.

With regard to the second aspect of JPL's position, we acknowledge DSN does not currently support transportation of goods and passengers in the same way NASA's Space Network, which handles communications for the International Space Station and other vehicles operating in low Earth orbit, does. Nevertheless, DSN plays a crucial role for command and control of spacecraft that perform essential Agency missions and are worth billions of dollars. For example, NASA used DSN to transmit command and control data for the Mars landing of the Curiosity Rover in 2012. As noted in the NIST guidance "Space operations are typically characterized by critical operational timing and safety parameters, and low tolerance for error. Unauthorized modification or destruction of time-critical information necessary to these functions may result in significant property loss and loss of human lives." Finally, looking ahead DSN will support future manned missions to an asteroid or Mars.

### *Disaster Monitoring and Prediction*

JPL also did not consider the NIST information type "Disaster Monitoring and Prediction" when categorizing DSN. JPL officials told us they did not include this information type in their assessment because DSN does not play a role in defense or national security operations. Moreover, officials assert DSN does not directly act as a warning system. However, NASA uses DSN to track near-Earth objects – comets and asteroids that pass within 28 million miles of Earth's orbit – to monitor potential threats to our planet.[25] Specifically, NASA uses the 70-meter antenna in Goldstone for radar observations to characterize the size and rotation and is currently observing and tracking about 75 near-Earth objects. Accordingly, because the Network supports identification and tracking for objects that could pose a threat to Earth, in our judgment, "Disaster Monitoring and Prediction" is an appropriate information type to consider when categorizing the DSN system.

[24] NIST Special Publication 800-60 Volume II, Section D.11, states that the category "Transportation" involves all federally supported activities related to the safe passage, conveyance, or transportation of goods and/or people. Impacts to some information and many information systems associated with transportation activities may affect the security of, not only the transportation infrastructure, but also to a broad range of other critical infrastructures and key national assets.

[25] NASA's Authorization Act of 2005 required the Agency to implement a "program to detect, track, catalog, and characterize the physical characteristics of near-Earth objects equal to or greater than 140 meters in diameter in order to assess the threat of such near-Earth objects to the Earth." The Act also amended the National Aeronautics and Space Act of 1958 and additionally required NASA to "provide warning and mitigation of the potential hazard of such near-Earth objects to the Earth." NASA OIG "NASA's Efforts to Identify Near-Earth Objects and Mitigate Hazards" (IG-14-030, September 15, 2014).

### *Similar Satellite Ground Control Systems Categorized as "High"*

We benchmarked the process JPL used to categorize DSN with the system security category determination process used by NASA's Space Network and a satellite ground system operated by the National Oceanic and Atmospheric Administration (NOAA). We found both the Space Network and NOAA included "Space Operations" in their categorization determinations and rated their systems as "High." NOAA also included "Disaster Monitoring and Prediction" in its determination.

In summary, DSN provides critical command and control capabilities for Agency assets worth billions of dollars and will support communications infrastructure for future manned deep space flights. Moreover, while the likelihood of a large diameter asteroid strike to Earth in the near future is low, the impact of such an occurrence could be catastrophic. Consequently, we believe it would be prudent for DSN to receive IT security protection associated with a "High" security category rating. During the audit, we consulted with the Acting Senior Agency Chief Security Officer at NASA, who agreed that DSN is used for command and control of Agency missions and plans to weigh the risks against the resources needed to redefine the system categorization.

## JPL IT Security Database Inventory was Inaccurate

NASA policy and NIST guidelines require the Agency to develop a system to account for information system components accurately. In FY 2003, JPL developed the Information Technology Security Database (Database) to maintain system security documentation and perform many security-related activities. The Database is the authoritative source for various DSN System Security Plans' hardware and software inventories and is used to support certification, accreditation, and ongoing authorizations of JPL systems, to make risk-based decisions, and for ensuring the appropriate security controls are applied to individual system components.[26]

We sampled 226 items from the Database, and found 106 (47 percent) contained inaccurate information.[27]

- 49 (22 percent) were marked as either active or inactive, but were either awaiting disposal or had already been excessed and therefore should have been removed from the Database.[28] This mischaracterization creates the burden of managing extensive, inaccurate lists - which was the case with the Plans we reviewed - and shifts focus from ensuring the proper controls have been appropriately applied.
- 21 (9 percent) listed as active were actually non-operational on JPL's systems. This creates a lack of situational awareness about an item's status.
- 19 (8 percent) were listed with the wrong property numbers, locations, and Internet Protocol addresses or could not be located during our walk through.

[26] DSN IT assets at JPL and the Complexes are governed by five System Security Plans, which govern flight hardware assets as well as administrative and mission support computing systems found at each of the key DSN Complexes.

[27] Using samples from the five System Security Plans, we performed onsite inventory validation checks at Goldstone, Madrid, and Canberra as well as the Exelis Monrovia, California, facility that houses DSN's Remote Operations Center network.

[28] "Active" refers to components operating on the network. "Inactive" refers to items no longer in use on the network or spares. "Excessed" refers to components planned for some form of disposal and ultimate removal from the JPL logistics property list.

- 10 (5 percent) were active on the wrong system and not covered by the appropriate System Security Plan. This could result in assets connected to the network without the appropriate controls and the possibility security controls would go unmonitored.
- 7 (3 percent) were listed as inactive but were identified as active on the system, which weakens overall situational awareness about an item's status and could lead to items connected to the network without the appropriate security controls.

An inaccurate asset inventory can lead to systemic problems over time, causing loss of valuable property and data and essentially undermining the efforts of other critical IT security processes.

After reviewing our results, DSN personnel agreed the processes used to capture and account for active network components needed attention and explained they have had problems ensuring appropriate personnel are notified when inventory modifications are made. Further, JPL also integrates logistics information in the Database; however, location and other fields were not specific enough and many times omitted, and there was limited integration with automated asset discovery tools in the inventory process. For example:

- DSN personnel are located in various geographic locations and utilize multiple systems to track computing assets for both accounting and IT security purposes. As such, the processes are not effectively integrated and communication channels between property stakeholders are overly complex.[29]
- During our visits, foreign personnel in Madrid and Canberra were not aware they had access to the Database to upload bulk changes and were relying on JPL personnel to make changes. This created opportunities for delays, errors, and omissions.
- Both IT security and JPL accounting elements are included in the Database, resulting in extensive inventory lists that are inefficient, difficult to manage, and undermine the intent of IT security. Further, in some cases NIST and NASA asset tracking elements were not included or inadvertently omitted in hardware inventories. For example, locations and responsible personnel were often blank or lacked detail.
- Contrary to NIST recommendations and IT security best practices to continuously monitor active network components, there is limited use of automated asset discovery tools to populate the Database.

Maintaining effective accountability of active hardware components on a large system or group of systems is a daunting task that requires effective administrative processes and technology. In our judgment, attempting to integrate logistics and IT security while maintaining appropriate information for each task makes IT security even more challenging.

Our review identified a series of factors that have resulted in extensive inventory inaccuracies that pose avoidable risk to JPL and NASA computing assets, data, and mission capability. Without effective asset tracking capabilities, the risk increases that something critical will be missed and assets and data needlessly exposed to compromise. While DSN personnel are now aware of the problems, and have begun researching solutions, until a solution is implemented NASA and DSN will continue to be at risk.

[29] Five entities are involved in populating the Database hardware inventory fields for tracking and accounting for components: JPL Logistics, JPL CIO Backup Services, DSN Logistics, Database users, and IBM Endpoint Manager. JPL Logistics is JPL's property accountability office; OCIO Backup is a feed from the institutional data backup system; Database users are individuals responsible for keeping the Database updated; and in some cases JPL's IBM Endpoint Manager software product provides the operating system and Internet Protocol address.

# Vulnerability Identification and Mitigation Practices were Inadequate and Not in Accordance with NASA Policy

During our review, we found 126 critical- and 1,069 high-impact vulnerabilities on DSN networks.[30] This condition occurred because Complex personnel did not follow NASA and JPL's vulnerability management policies associated with credentialed scanning on the DSN Flight Network and the DSN administrative support networks at all three Complexes, as well as at Exelis' Monrovia, California, facility.[31]

## NIST Vulnerability Process

NIST recommends agencies run vulnerability-scanning tools on all network systems and deliver prioritized lists of the most critical vulnerabilities to responsible system administrators. Agencies should also use a Security Content Automation Protocol-validated vulnerability scanner that looks for both code- and configuration-based vulnerabilities.[32] Further, the Agency should perform vulnerability scanning in an authenticated or credentialed mode.[33]

## Credentialed Scanning

Credentialed scanning can identify critical vulnerabilities residing on a system or network not revealed by non-credentialed scans.[34] For example, in a 2011 audit of NASA's continuous monitoring program, we identified a significant number of vulnerabilities by running credentialed scans on systems that NASA had previously subjected only to non-credentialed scans.[35] Although the credentialed scans were performed on only a small sample of Agency components, we identified 2,644 high-impact vulnerabilities compared with 59 high-impact vulnerabilities identified by the non-credentialed scans.

[30] The terms "critical-" and "high-impact" correlate to vulnerability ratings identified in the Department of Homeland Security's National Vulnerabilities Database common vulnerabilities scoring system and depict the respective level of harm to systems.

[31] The DSN Flight Network is governed by JPL IT System Security Plan 11. The administrative support networks at Madrid, Canberra, and Goldstone Complexes and the Monrovia facility are governed by JPL IT System Security Plans 390, 454, 542, and 455 respectively. JPL limited our credentialed scanning of Plan 11 to 8 components due to operational impact concerns.

[32] Security Content Automation Protocol is a method for using specific standards to enable automated vulnerability management, measurement, and policy compliance evaluation (i.e., FISMA compliance).

[33] A credentialed scan uses administrator rights on the target host while a non-credentialed scan does not. Administrator rights are permissions granted to users allowing them to view installed software and to make changes to computer system configurations.

[34] 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 accessing the car's engine.

[35] NASA OIG, "NASA Faces Significant Challenges in Transitioning to a Continuous Monitoring Approach for Its Information Technology Systems" (IG-12-006, December 5, 2011).

In response to the 2011 audit, NASA began requiring quarterly credentialed scanning of IT assets in 2012.[36] JPL policy is even stricter – requiring monthly credentialed scanning of JPL network components. However, we found JPL was not performing credentialed scanning on its DSN systems and DSN system administrators were unaware of the requirement to do so.[37]

During the audit, we requested and JPL IT Security agreed to perform credentialed scanning on a sample of 74 components.[38] The credentialed scans identified a large number of critical and high vulnerabilities. Specifically, the 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.

Comprehensive vulnerability management is a fundamental element of managing IT security risks and a proven means of reducing the severity and success of attacks and for saving organizational resources responding to such attacks. A 2014 Global Threat Intelligence Report states that organizations with a comprehensive and mature vulnerability management program are four times less susceptible to attacks and have as many as four times fewer exploitable vulnerabilities and 20 percent faster remediation times than organizations not using these capabilities.[39] In addition, NASA recently performed vulnerability identification and penetration testing on some of its systems, which resulted in identification and mitigation of numerous remotely exploitable vulnerabilities. NASA estimated these efforts will save it as much as $28.4 million.[40] Moreover, a study of JPL's IT security programs, including those associated with DSN, requested by MAVEN officials identified weaknesses in JPL's vulnerability management program. In response to the study, JPL officials stated the view that performing credentialed scanning would be a management burden and that the cost of implementing such an approach would outweigh any risks associated with unidentified vulnerabilities.[41] We disagree. Although not all vulnerabilities identified during scanning present an actual risk, credentialed scanning is a crucial tool in managing risks to systems and data.

[36] ITS-HBK-2810.04-01A "Security Categorization, Risk Assessment, Vulnerability Scanning, Expedited Patching, & Organizationally Defined Values," October 12, 2012.

[37] Vulnerability scanning can be done over the network without using credentials or by using credentials that log into individual components to gather comprehensive security-related information about the individual component.

[38] JPL IT Security declined to allow credentialed scanning on most of the components from the Flight Network for fear the system would experience a loss of availability if the scanner were to negatively interfere with control system processes or overtax the resources available on control system components. As a result, only 8 of the 74 components were from the Flight Network System Security Plan.

[39] NTT Group's Innovation Institute collected and analyzed approximately three billion actual attacks from trillions of data logs in order to produce the findings for the 2014 Global Threat Intelligence Report.

[40] NASA based the savings on the number of vulnerabilities the team was able to exploit during testing using the costs expressed in the NTT Group's 2014 Global Threat Intelligence Report.

[41] Department of Energy, Office of Security and Cyber Evaluations, "Independent Oversight Review of the Jet Propulsion Laboratory Information Technology Security Program," June 3, 2013.

# JPL Not in Compliance with Federal and NASA Security Configuration Baseline Application Requirements

Although JPL applies limited protective configuration measures, we found those measure do not meet Federal or NASA requirements. JPL personnel told us they do not follow these requirements because the JPL prime contract does not require they do so.

## Requirement for United States Government Configuration Baseline

In 2007, the Office of Management and Budget issued a memorandum requiring Federal agencies to apply a standard configuration baseline to IT components running specific operating systems on their networks.[42] Now known as the United States Government Configuration Baseline (USGCB), the requirements apply both to Federal agency systems and Government-owned but contractor-operated systems, such as DSN.

Security baselines include a group of configuration settings important for hardening components so they are less vulnerable to potential attackers. As the name suggests, the settings provide a static baseline to monitor for any unusual activity that could indicate malicious activity is taking or has taken place. The security settings included in USGCB range from disabling unneeded and potentially vulnerable services to ensuring passwords are sufficiently complex. Malicious attackers will target vulnerable services or repeatedly guess passwords in attempts to gain unauthorized access to networks or systems.[43] Once an intruder gains access, they can then probe for other components on the network with open configurations that, if not hardened with the proper baseline settings, may allow further intrusion into the network.

## OIG Testing Showed Non-Compliance

We tested compliance with USGCB requirements on DSN computer components utilizing JPL's software tools. We selected 32 DSN computer components from 3 of DSN's System Security Plans and tested them for compliance with USGCB standards.[44]

We found none of the 32 components complied with USGCB and that on average 170 out of 260 (65 percent) security checks failed when testing for compliance against the standards. For example, the Federal standard for a password is a minimum of 12 characters, while JPL only uses an 8-character minimum. Other non-compliant settings included requiring passwords be changed every 90 days rather than the 60-day Federal standard.

[42] For other operating systems including Windows server, UNIX, and Linux, a NASA team has developed applicable baselines based on Government and industry best practices. JPL does not leverage the use of these, but rather utilizes its own protective measures.

[43] Brute force attacks involve guessing what a password may be a character at a time. The concept is that if an attacker guesses enough times they will eventually find a match, hence the longer and more complex a password is, the harder it will be and longer it will take for an attacker to succeed in guessing. Brute force attacks can be done manually or with widely available password cracking tools.

[44] Examples of the USGCB configuration settings include minimum password size, forced computer hibernation, and disabling unnecessary and potentially vulnerable services.

JPL does apply some security settings, but they are not as robust a set of controls as the Federal baseline and therefore, in our judgment, do not meet the intent of the USGCB standard. For example, JPL's protective measures for the Microsoft Windows 7 operating systems includes 26 rules, while the USGCB standard for Windows 7 includes at least 260 configuration settings.

High profile intrusions have occurred in recent years at JPL by attackers circumventing JPL's IT security program. OIG investigations of some of these intrusions identified missing password controls, compromise of account credentials, and attempts to further infiltrate systems using password-cracking tools, all of which highlight the need for robust and stringent settings. By not applying and monitoring USGCB on individual computing components and operating systems, JPL is not meeting the intent of Federal or NASA standards and exposing NASA systems and data to undue risk of compromise.

## Gaps Existed in NASA's Network Monitoring and Incident Reporting Capabilities

JPL is required to report computer security incidents on its network to the NASA SOC, which is responsible for monitoring Agency network traffic for suspicious activity and performing any needed investigation.[45] We found that although JPL reports computer security incidents to the SOC and the OIG, NASA lacks the ability to verify the accuracy or completeness of JPL's reporting.[46] Further, we found JPL has network connections that NASA is not monitoring because JPL and NASA have not come to an agreement on comprehensive monitoring. As a result, NASA lacks the ability to monitor a large portion of JPL network traffic – which may be destined for or originate from DSN associated components – for suspicious activity, provide timely assistance in the event of an incident, and ensure its information systems and data are fully protected.

NIST guidelines recommend agencies employ automated mechanisms to assist in tracking computer security incidents and collecting and analyzing incident information. The guidelines also require personnel to report suspected security incidents to the organization's incident response capability within defined time periods. NIST specifically notes the importance of incident management:

> "Preventive activities based on the results of risk assessments can lower the number of incidents, but not all incidents can be prevented. An incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring IT services. . .Continually monitoring for attacks is essential. . .It is also vital to build relationships and establish suitable means of communication with other internal groups."[47]

[45] Located at Ames Research Center, NASA's SOC operates continuously and has 39 dedicated IT security personnel.

[46] In accordance with its contract, JPL is required to report any type of IT security incident that might have Agency security implications to the NASA SOC, NASA OIG, and NASA Management Office in a timely manner.

[47] NIST Special Publication 800-61, Revision 2, "Computer Security Incident Handling Guide," August 2012.

To support compliance with NIST, NASA developed an Incident Response and Management Plan and established the SOC to conduct network monitoring, manage response and investigative activities, and report incidents to the United States Computer Emergency Readiness Team.[48]

The NASA SOC monitors each Center's network activity 24 hours per day, 7 days a week for suspicious or malicious network activity using strategically placed sensors and dedicated IT security staff. Because of this robust capability, the SOC is able to develop a knowledge base of past incidents and proactively develop signatures for real-time monitoring of internet protocol packets, and immediately respond to suspicious or malicious activity. Conversely, JPL's SOC is staffed by dedicated personnel only during normal business hours and actively monitors network activity through strategically placed sensors on JPL connections. In the event an alarm is triggered after hours, JPL employs automated means for identifying malicious activity and has personnel on call in the event such activity is identified. JPL implemented these capabilities because of a 2011 intrusion that resulted in JPL systems being compromised for nearly a year undetected.

Previous incidents, including the 2009 intrusion on DSN support systems, have highlighted the need for more comprehensive monitoring from the NASA SOC of JPL's networks. Following the intrusion, the Deputy CIO stated the OCIO would work with the NASA Management Office to implement more specific security requirements, including network monitoring that affords NASA SOC complete visibility of JPL network traffic through the use of intrusion detection sensors and network flow tools. However, the Agency has yet to implement this change.

JPL also maintains two communication links over which NASA has no visibility. Specifically, JPL has three communications trunks over which information is exchanged in support of both JPL and NASA operations: a 40-gigabit connection to its local communication's provider and two 1-gigabit connections managed by NASA's Communications Service Office.[49] The NASA SOC has visibility only into one of the 1-gigabit connections and is therefore unable to validate JPL's reporting or assist in the mitigation or investigation of any suspicious or malicious activity that may take place on the much larger connection and the other smaller NASA connection. In our judgment, by not having these capabilities in place, NASA is not fully utilizing valuable resources and malicious activity is more likely to happen undetected.

[48] 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.

[49] The Communications Service Office provides wide area network services, which directly support the Human Exploration and Operations, Science, and Aeronautics Mission Directorates, all NASA Centers and facilities, Agency institutional activities, and many projects and missions.

# PHYSICAL SECURITY REQUIREMENTS WERE NOT CONSISTENTLY IMPLEMENTED ACROSS DSN COMPLEXES

We found required physical security controls were missing or inconsistently implemented at Goldstone, Madrid, and Canberra; procedures to assign FSL designations were not in compliance with NASA policy; and NCI facility security assessments had not been completed. Furthermore, physical security waivers or other risk acceptance documentation were not consistently in place for the missing controls. As a result, NASA's domestic and foreign DSN facilities may be unnecessarily vulnerable to compromise.

## NCI Requirements

Every Federal agency is required to establish a program to identify critical essential infrastructure and key resources, evaluate these assets for vulnerabilities, and fund and implement appropriate security enhancements, both procedural and physical, to mitigate vulnerabilities.[50] NASA has appropriately designated DSN as NCI because of its importance to NASA missions. Agency policy states that NCI facilities shall be rated and protected at a minimum FSL III level, which mandates such items as controlling access through the use of intrusion detection systems, electronic physical access control systems, and closed circuit television.

## Goldstone

We found that physical security at Goldstone does not meet NASA requirements for an FSL III facility. During a visual inspection of the Complex, we found several discrepancies related to intrusion detection systems around NCI antenna sites, as well as insufficient monitoring protection for supporting infrastructure such as heating, ventilating, and air conditioning systems and backup power generation. We also reviewed the security assessments JPL performed on Goldstone and found the documents did not meet the intent of facility security assessment guidelines in NASA policy. For example, documented NCI physical security assessments were not available and NCI designated antenna infrastructure was improperly assigned an FSL II designation. DSN raised the antenna infrastructure designation to an FSL III after we informed DSN officials of the results of our review.

Because Goldstone is located in a remote location on the Fort Irwin military base, we requested any waivers on file for requirements such as perimeter intrusion detection. In response, JPL provided us with waivers for security guard response time, fencing, and perimeter intrusion detection. However, risk acceptance or waiver documentation was not available for the other discrepancies we identified such as the lack of intrusion detection system around antenna structures or package screening.

[50] NPR 1600.1A, "NASA Security Program Procedural Requirements."

We also appreciate that NASA's physical security requirements for facilities and property are relatively new mandates developed in 2012, and that JPL had a relatively short time to adjust and implement these mandates prior to our review. Improved coordination with NASA OPS and NASA Management Office should help Goldstone's contractor perform an appropriate facility security assessment and identify the baseline level of protection requirements and the achievable level of protection.

## Madrid and Canberra

We found that assets located in foreign countries presented unique security considerations for both NASA and JPL. Madrid and Canberra are remote and relatively inconspicuous facilities governed by local laws and regulations, many of which differ significantly from NASA requirements. This can present challenges when assessing the facilities' security posture and determining exactly which controls should be implemented or if other mitigations meet the intent of NASA requirements.

Our limited physical security assessments identified discrepancies for protecting NCI at the foreign Complexes. For example, we found DSN antenna structures in Canberra were not enclosed with fencing or protected by intrusion detection systems or electronic access controls. Although Canberra had a site-wide closed circuit television with central monitoring in the guard station and a single perimeter fence with intrusion detection system, these measures did not prevent visiting contractors from walking directly to unprotected antenna structures. In contrast, we observed double perimeter fencing around the entire Complex and fencing and a physical access control system for antenna structures at Madrid, measures that more closely align with NASA requirements. Moreover, consistent with Australian law, Canberra security guards were unarmed while guards at Madrid were armed.

Although the Madrid and Canberra Complexes are located about 20 to 30 miles from populated urban areas, security officials we met with in Spain and Australia suggested this does not negate the need for comprehensive physical security controls. Further, NASA Management Office officials stated Madrid has a better security posture due to Spain's willingness to accept physical security requirements. Further, NASA's Contracting Officer was aware of the inconsistencies in physical security controls and cited difficulties negotiating physical security requirements with CSIRO. In our judgment, identifying and documenting the challenges associated with managing NCI not only in the U.S., but also at foreign sites would permit NASA to better understand its vulnerabilities and where it should apply resources to mitigate significant security risks.

# NASA's Oversight of DSN's Foreign Contract Costs was Inadequate

NASA has not required the contractor that operates Madrid to provide detailed cost support on a timely basis or ensured the Defense Contract Audit Agency (DCAA) performs incurred cost audits of the Madrid and Canberra contracts on a routine basis. As a result, NASA cannot ensure that approximately $36.6 million in annual payments made to the contractors responsible for operating and maintaining Madrid and Canberra are accurate.

## Reporting and Oversight Requirements in Foreign Contracts

NASA entered into contracts with INTA and CSIRO that delineate the contractors' reporting and billing requirements and audit responsibilities. The Madrid contract requires INTA or its representative submit monthly financial status reports that include actual expenditures and estimates to complete planned operations and maintenance tasks for the current fiscal year within 30 days of the end of each month. INTA can request an advance payment for expenses; however, the payments should not exceed $5 million at any time. The Canberra contract requires CSIRO to submit monthly financial status reports that detail the actual expenditures during the reporting period within 15 days of the end of each month. CSIRO can request an advance payment with the submission of certified invoices and with the approval of the NASA Management Office. However, the payments should not exceed $5 million at any time.

Both contracts provide for the same audit requirements. Specifically, the Contracting Officer or an authorized representative, such as DCAA, has the right to examine and audit supporting records for reported costs.[51] In addition, the contractor may submit an invoice or voucher supported by a statement certifying the claimed allowable cost for performing the contract in such form and detail as the representative may require.[52] Finally, the Contracting Officer has the right to request an audit of the invoices or vouchers at any time.

## NASA Signed Madrid Contractor Invoices without Timely Detailed Cost Submissions

NASA failed to ensure ISDEFE (INTA's representative) provided timely support for claimed costs. In accordance with the contract, ISDEFE is required to provide monthly financial status reports that summarize actual expenditures within 30 days of the end of the month. However, neither ISDEFE nor its predecessor have consistently provided these reports, and, in fact, some submissions have been up to 6 months late. NASA personnel told us Madrid invoices are routinely approved for payment without detailed support because advance payments are authorized and JPL monitors the contractor's work.

[51] Federal Acquisition Regulation 52.215-2(e), "Audit and Records – Negotiation."

[52] Federal Acquisition Regulation 52.216-7(a), "Allowable Cost and Payment."

DSN assures the Agency that ISDEFE has completed the technical work and mission support requirements have been fulfilled. Nonetheless, NASA personnel admit that the lack of detailed monthly financial reports prevent them from ensuring costs are reasonable in a timely manner.

## Timely DCAA Audits Not Performed on Foreign Contracts

NASA has also failed to ensure DCAA audits are performed consistently and timely on the approximately $36.6 million in annual costs on the foreign contracts. DCAA incurred cost audits assist procurement and contract administration personnel by providing information or advice as to whether contractor costs are allocable, allowable, and reasonable. The information is based on an analysis of the contractor's estimated and incurred costs, a review of the contractor's cost control systems, and other analyses and reviews of the contractor's financial and accounting records. Procurement and contract administration personnel also use DCAA services to assist in the negotiation, administration, and settlement of contracts.

However, our review noted a failure by NASA and DCAA to conduct an appropriate number of audits and deficiencies in those that were performed. For example, NASA lacks incurred cost audits for ISDEFE's FYs 2011 through 2013 costs for the Madrid contract. During our audit, NASA informed us that DCAA plans to perform incurred cost audits on Madrid's FY 2011 and 2012 costs during FY 2015. Further, in 2006, NASA requested DCAA evaluate an audit CSIRO and the Australia National Audit Office performed on CSIRO's incurred costs for the Canberra contract.[53] In that report, DCAA advised NASA's Contracting Officer to request DCAA perform annual incurred costs audits of CSIRO. Also at the time of the audit, CSIRO had subcontracted out the operation of Canberra; however, in an effort to reduce costs, CSIRO made the decision to operate the Complex itself beginning in 2010. In 2012, DCAA reported on CSIRO's accounting system and concluded it was inadequate for accumulating and billing costs under Government contracts.[54] As of February 2014, NASA has not requested DCAA perform an audit of CSIRO's FYs 2012 through 2013 incurred costs.[55]

As we reported in December 2014, DCAA has a substantial backlog of incurred cost proposals awaiting audit, including approximately 1,153 proposals relating to NASA contracts.[56] Accordingly, NASA cannot afford to rely solely on DCAA to determine whether incurred costs are allocable, allowable, and reasonable, and based on our 2014 report agreed to revise the Agency's current processes or develop additional procedures and oversight mechanisms to better safeguard contract funding, including seeking alternatives to DCAA-type incurred cost audits.[57] Similarly, we found that the Contracting Officer for the foreign contracts did not annually request the DCAA audits or perform additional oversight to ensure the appropriateness of contractor costs in the absence of those audits. Without detailed costs and monthly invoices available for review, coupled with consistent DCAA audits, NASA cannot ensure that annual costs of approximately $36.6 million are allocable, allowable, and reasonable.

[53] DCAA, "Evaluation of an Audit performed by CSIRO and Australian National Audit Office," August 1, 2006.

[54] DCAA, "Independent Audit of Commonwealth Scientific and Industrial Research Organisation's Postaward Accounting System," February 21, 2012.

[55] On February 4, 2015, DCAA notified CSIRO that its incurred cost proposals were inadequate, and CSIRO must correct the deficiencies and resubmit the proposals.

[56] NASA OIG, "Costs Incurred on NASA's Cost-Type Contracts" (IG-15-010, December 17, 2014).

[57] Currently, the NASA Federal Acquisition Regulation Supplement 1815.404-2(a)(1)(F)(1), "Data to Support Proposal Analysis-Use of Contractor to Perform Contract Audit Services," states that at contractor locations where DCAA currently conducts any contract audit services the use of a contractor to perform contract audit services is not allowed.

# CONCLUSION

DSN is a central component of the Agency's space communications and navigation capability and provides essential services to Agency missions as well as missions of NASA's international partners. The success of the Network depends upon a global system of antennas and supporting infrastructure that requires maintenance, replenishment, modernization, and protection. Moreover, the Agency's plans to send humans into deep space will add demands on the Network. Given the age and conditions of DSN's physical infrastructure, it is essential the Network's DAEP modernization plan is implemented to meet current and future operational commitments.

Reduced budgets for DAEP since FY 2013 have forced NASA to delay or cancel completion of key upgrades and sustainment efforts. To its credit, the Network has effectively managed risks associated with these cuts and adjusted capabilities to meet cost, schedule, and performance goals. However, if budget reductions continue, we are concerned DAEP could face additional delays, which could ultimately hinder its ability to meet future operational commitments. Developing complete cost estimates for DAEP is a key step in determining, planning, and justifying the budgets necessary to meet these operational commitments. To date, NASA has not updated a comprehensive life-cycle cost estimate to ensure DAEP will be implemented and all operational needs will be met. Further, NASA lacks the proper oversight of the approximately $36.6 million in annual costs for the foreign operations because the Contracting Officer failed to ensure detailed cost support was provided on a timely basis or request timely DCAA audits.

We also identified significant deficiencies and needed improvements in the management of DSN's IT and physical security contractual requirements. Fundamental to this effort is an improved partnership between NASA and JPL to ensure NASA maintains consistent practices across DSN that align with current and evolving Federal standards. DSN's upcoming authorization cycle provides JPL with an opportunity to comply with Agency requirements and Federal guidelines.

With regard to physical security, we found required controls were missing or inconsistently implemented at Goldstone, Madrid, and Canberra and procedures used to assign FSL designations were wrong and NCI facility security assessments had not been completed. Furthermore, physical security waivers or other risk acceptance documentation were not consistently in place for the missing controls. Given the continuing threat of terrorist activity facing the United States and our partner countries supporting DSN, it is crucial NASA ensure physical security measures are appropriately applied to its critical infrastructure and the management of these protections provides a consistent situational awareness in these challenging environments.

We acknowledge the difficulty NASA faces implementing both IT and physical security controls given funding, legal, and other constraints. However, to the extent these challenges hinder NASA's ability to meet mandated security requirements for DSN and its supporting networks and infrastructure, the Agency should document the reasoning and identify the factors or compensating controls that are driving deviations from established guidance.

# RECOMMENDATIONS, MANAGEMENT'S RESPONSE, AND OUR EVALUATION

In order to obtain a realistic, accurate, and transparent budget that supports DSN's ability to provide required communication services, we recommended the Deputy Associate Administrator for SCaN:

1. Direct DSN to develop a detailed life-cycle cost and schedule estimate for DAEP that takes into consideration realistic savings from planned efficiency measures.

In order to ensure DSN follows established IT security policies, standards, and governance methodologies, we recommended the NASA CIO and NASA's Chief Information Security Officer work with the JPL CIO through the Contracting Officer to:

2. Ensure DSN's Plan 11 system security categorization analysis takes into consideration NIST Space Operations and Disaster Monitoring and Prediction information types and update IT security controls consistent with the appropriate security impact level.

3. Direct DSN IT security personnel to review the information in the five DSN System Security Plans and update them to reflect accurate information.

4. Establish internal controls to ensure DSN IT components are accurately entered and characterized and maintained in the Information Technology Security Database.

5. Ensure the JPL CIO develops detailed processes for ensuring credentialed scanning of JPL IT System Security Plan's 390, 454, 455, and 542 components. At a minimum, this should include (1) instructions for analyzing results of scans to ensure authentication was successful; (2) determination of mitigation processes for identified vulnerabilities; (3) identifying Plan 11 components that can undergo credentialed scanning without impacting operations; and (4) developing a formal risk acceptance or wavier process for those components that cannot undergo a credentialed scan due to operational constraints.

6. Direct JPL to follow Federal and NASA requirements for security configuration baselines on all JPL-managed system components and if necessary, document deviations through a formal risk acceptance process or waivers.

7. Take steps to ensure the NASA SOC has appropriate oversight at JPL to support NASA's Agency-wide incident management program.

In order to ensure the physical security requirements for NCI are implemented consistently across the DSN Complexes, we recommended the Assistant Administrator for Protective Services in conjunction with the Contracting Officer

8. Review and update the contracts with Madrid and Canberra to include physical security requirements for NCI as stated in NASA policies.

9. Perform facility security assessments in accordance with NASA policy and identify the appropriate FSL for NCI facilities at Goldstone, Madrid, and Canberra and document deviations from NASA policy using the formal risk acceptance process or waivers to requirements by the Assistant Administrator for OPS.

Due to the dynamic nature of technology and a constantly changing threat landscape, we recommended the CIO and the Assistant Administrator for Protective Services in conjunction with the NASA Chief Information Security Officer and Contracting Officer

10. Develop a strategy for implementing evolving Federal IT and physical security policies at JPL through means that minimize time-consuming negotiation of formal contract modifications.

In order to improve NASA's oversight for the allocable, allowable, and reasonable costs on the DSN foreign contracts, we recommended the Deputy Associate Administrator for SCaN in conjunction with the Contracting Officer

11. Require INTA's representative to submit the required detailed monthly financial status reports.

12. Request DCAA perform incurred cost audits on the Madrid and Canberra contracts, and if DCAA cannot perform the audits in a timely manner, seek an alternative contract audit service.

We provided a draft of this report to NASA management, who concurred with our recommendations and described planned corrective actions. Because we consider management's proposed actions responsive to our recommendations, the recommendations are resolved. We will close the recommendations once the actions are completed and we have verified the actions are sufficient to ensure compliance. Management's full response to our report is reproduced in Appendix B. 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; Jim Griggs, Team Lead; Barbara Moody, Auditor; Christopher Reeves, IT Specialist; Earl Baker, Legal Counsel; and Benjamin Patterson, Editor.

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.

Paul K. Martin
Inspector General

# APPENDIX A: SCOPE AND METHODOLOGY

We preformed this audit from May 2014 through February 2015 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.[58] In May 2014, we initiated our audit of DSN to examine the extent to which (1) DSN is positioned to meet its current and future commitments, (2) DSN is managing IT and physical security risks, and (3) NASA is administering foreign contracts.

To evaluate the extent that DSN is positioned to meet current and future commitments we evaluated Agency policy and guidance on management and utilization of NASA's space communication and navigation infrastructure; determined whether NASA effectively managed DAEP within cost, schedule, and performance goals; and whether NASA effectively planned for current and future DSN funding requirements. For our evaluation, we reviewed:

- contract documents, monthly financial status reports, annual operating plans, and budget target ceilings for the Goldstone, Madrid, and Canberra Complexes;
- DAEP's September 2010 Implementation Plan, April 2012 Phase I Implementation Plan, FYs 2009 through 2025 life-cycle cost spreadsheets, actual costs from FYs 2009 through July 2014, and the lessons learned document from the first two antenna builds; and
- DSN's FYs 2009 through 2018 planned efficiency savings to fund DAEP; planned mitigation for FYs 2014 through 2019 budget cuts; FY 2014 upgrade and sustaining projects status; FYs 2012 through 2016 planning, programming, budgeting, and execution submissions; October 2009, 2010, 2011, 2012, and May 2014 project status reviews; current and future mission requirements; FYs 2009 through 2014 performance metrics; funding process overview; FYs 2013 through 2015 reimbursable funds received; and FYs 2009 through 2013 planned and actual maintenance and operations costs and deferred maintenance.

In addition, we interviewed management and personnel from DSN, the SCaN Program, NASA Management Office, JPL Interplanetary Network Directorate, Goldstone Complex, Madrid Complex, and Canberra Complex. We also reconciled and traced DSN's financial reports to JPL's official books and records.

To evaluate how DSN is managing IT and physical security risks, we reviewed relevant industry studies, best practices, and reports. We benchmarked DSN's system security categorization process to NASA's Space Network and NOAA's methodology. We also reviewed relevant Federal, NASA, and JPL mandates, standards, guidance, and policy documents related to IT and physical security, including:

[58] As of the date of this report, we have issued NASA OIG, "Space Communications and Navigation: NASA's Management of the Space Network" (IG-14-018, April 29, 2014) and "Audit of the Space Network's Physical and Information Technology Security Risks" (IG-14-26, July 22, 2014).

- FISMA and Homeland Security Act;
- Presidential policy directives;
- FIPS publications;
- NIST 800-series publications;
- Office of Management and Budget and Federal CIO Council guidance on USGCB
- NASA Procedural Requirements, NASA Policy Directives, and NASA's IT Security Handbook;
- IT security policies and requirements; and
- JPL, Goldstone, Madrid, and Canberra contracts and task description documents.

We utilized the five System Security Plans JPL provided on May 21, 2014, to evaluate the IT security posture of DSN at JPL, Goldstone, Madrid, Canberra, and the Remote Operations Center. To evaluate IT security, we judgmentally selected active and inactive components from the security plans to validate the inventory, perform vulnerability scanning, and check for USGCB compliance. To determine if the information in the Database was accurate, we selected a sample of 160 active components from a universe of 1,460 active components and a sample of 66 inactive components from a universe of 1,218 inactive components from the five security plans. If possible, we physically observed the location of the component and compared its status to the Database. For credential vulnerability scanning and USGCB compliance testing, we selected a sample of 88 active components from the universe of 1,460 active components from the Goldstone, Madrid, and Canberra administrative support networks and the Remote Operations Center network. We utilized JPL's software tools to perform the scanning and baseline compliance testing and analyzed the results. We were only able to observe vulnerability scanning on eight DSN Plan 11 Flight Network components due to operational constraints.

We evaluated DSN's physical security posture by reviewing NCI protection program requirements related to the Agency's FSL assessments and compared it to JPL's security assignments for Goldstone. We also requested and reviewed waivers to requirements on disclosed deficiencies. We tested each Complex's compliance for NCI protection by visual observations and verification during our site visits. We discussed physical security controls and inconsistencies we found with personnel in NASA Management Office, OPS, and with the Regional Security Offices within the U.S. Embassy in Madrid and Canberra.

To evaluate the extent that NASA is administering DSN's foreign contracts, we reviewed the relevant Federal Acquisition Regulation clauses, and DCAA audit reports on Madrid and Canberra Complexes' financial statements, accounting systems, incurred costs, and invoicing. We also interviewed personnel in NASA's Contract and Grant Policy Division and the DCAA Liaison to determine the status and timeline for future DCAA audits.

To obtain an understanding of how advance payments to the Madrid and Canberra Complexes are approved and distributed and how the contractors billing for services are approved and paid, we reviewed the contracts and interviewed the Executive Assistant to NASA's Madrid Complex representative and Canberra Complex representatives. To determine whether the foreign Complexes are reporting accurate expenditures, we reviewed Madrid and Canberra's financial status reports and annual operating plans. We tested the accuracy of the financial status reports by tracing a selected sample of transactions in the report to the contractor's official books and records and verified that the billings reconciled.

# Use of Computer-Processed Data

We relied on computer-processed data such as budget data, annual operating plans, financial management reports, life-cycle cost estimate spreadsheets, 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 for our conclusions because we were able to assess the data. For example, we reconciled the financial data provided 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 5 years, the NASA OIG issued five reports and one testimony of significant relevance to the subject of this report. Unrestricted reports can be accessed at http://oig.nasa.gov/audits/reports/FY15/index.html. In addition, GAO issued two reports of significant relevance, which can be accessed at http://www.gao.gov.

### *NASA Office of Inspector General*

*Costs Incurred on NASA's Cost-Type Contracts* (IG-15-010, December 17, 2014)

*NASA's Efforts to Identify Near-Earth Objects and Mitigate Hazards* (IG-14-030, September 15, 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)

*NASA Cybersecurity: An Examination of the Agency's Information Security*, Testimony before the Subcommittee on Investigations and Oversight, House of Committee on Science, Space, and Technology (February 29, 2012)

### *Government Accountability Office*

*NASA: Actions Needed to Improve Transparency and Assess Long-Term Affordability of Human Exploration Programs* (GAO-14-385, April 27, 2006)

*NASA's Deep Space Network: Current Management Structure is Not Conducive to Effectively Matching Resources with Matching Resources with Future Requirements* (GAO-06-445, April 27, 2006)

# APPENDIX B: MANAGEMENT COMMENTS

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

MAR 24 2015

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: Response to Office of Inspector General (OIG) Draft Audit Report, "NASA's Management of the Deep Space Network" (Assignment No. A-14-012-00)

NASA appreciates the opportunity to review your draft report entitled "NASA's Management of the Deep Space Network" (Assignment No. A-14-012-00), dated February 24, 2015.

In the draft report, the OIG makes 12 recommendations intended to improve performance levels and future reliability of the Deep Space Network (DSN) Program. NASA's response to the OIG's recommendations, including planned corrective actions, follows:

In order to obtain a realistic, accurate, and transparent budget that supports DSN's ability to provide required communication services, the OIG recommends that the Deputy Associate Administrator for Space Communications and Navigation (SCaN):

**Recommendation 1:** Direct DSN to develop a detailed life-cycle cost and schedule estimate for the Deep Space Network Aperture Enhancement Project (DAEP) that takes into consideration realistic savings from planned efficiency measures.

**Management's Response:** Concur. NASA will ensure a detailed life-cycle cost and schedule estimate for the DAEP that takes into consideration realistic savings from planned efficiency measures will be requested in the Program and Resources Guidance (PRG) for each yearly Planning, Programming, Budgeting and Execution (PPBE) cycle and that this information is provided for each PPBE review.

**Estimated Completion Date:** Completed. This data has already been provided for PPBE-17 (the current PBE) and will be requested annually via the PRG guidelines.

In order to ensure DSN follows established IT security policies, standards, and governance methodologies, the OIG recommends that the NASA Chief Information Officer (CIO) and NASA's Chief Information Security Officer work with the Jet Propulsion Laboratory CIO through the Contracting Officer to:

**Recommendation 2:** Ensure DSN's Plan 11 system security categorization analysis takes into consideration National Institute of Standards and Technology (NIST) Space Operations and Disaster Monitoring and Prediction information types and update Information Technology (IT) security controls consistent with the appropriate security impact level.

**Management's Response:** Concur. The NASA CIO will work, in conjunction with the Deputy Associate Administrator for SCaN, the NASA Management Office (NMO), and the JPL CIO, to ensure the controls assigned to the DSN's Plan 11 system security plan are appropriately reviewed to ensure alignment with NASA and JPL protection and risk management frameworks.

**Estimated Completion Date:** Expected completion date for this activity is September 30, 2015, contingent on analysis of the contract and availability of resources.

**Recommendation 3:** Direct DSN IT Security personnel to review the information in the five DSN System Security Plans and update them to reflect accurate information.

**Management's Response:** Concur. The NASA CIO will work, in conjunction with the Deputy Associate Administrator for SCaN, the NMO, and the JPL CIO, to validate and, where necessary, enhance processes that will ensure that the information within all security plans is current and revalidated as required by the Authorization and Accreditation policy.

**Estimated Completion Date:** Expected completion date for this activity is July 31, 2015, contingent on analysis of the contract and availability of resources.

**Recommendation 4:** Establish internal controls to ensure DSN IT components are accurately entered and characterized and maintained in the Information Technology Security Database.

**Management's Response:** Concur. The NASA CIO will work, in conjunction with the Deputy Associate Administrator for SCaN, the NMO, and the JPL CIO, to ensure that processes and systems are in place to capture and continuously update the Security Database used to support JPL's risk management process.

**Estimated Completion Date:** Expected completion date for this activity is January 15, 2016, contingent on analysis of the contract and availability of resources.

**Recommendation 5:** Ensure the JPL CIO develops detailed processes for ensuring credentialed scanning of JPL IT Security Plan's 390, 454, 455, and 542 components. At a minimum, this should include (1) instructions for analyzing results of scans to ensure authentication was successful; (2) determination of mitigation processes for identified vulnerabilities; (3) identifying Plan 11 components that can undergo credentialed scanning without impacting operations; and (4) developing a formal risk acceptance or

wavier process for those components that cannot undergo a credentialed scan due to operational constraints.

**Management's Response:** Concur. The NASA CIO will work, in conjunction with the Deputy Associate Administrator for SCaN, the NMO, and the JPL CIO, to ensure that the needed insight and oversight is implemented to validate the scanning of assets on the DSN. This includes measuring, reviewing, verifying, monitoring, facilitating, and remediating to ensure coordinated and consistent cybersecurity implementation and reporting across all organizations without impeding local missions.

**Estimated Completion Date:** Expected completion date for this activity is January 29, 2016, contingent on analysis of the contract and availability of resources.

**Recommendation 6:** Direct JPL to follow Federal and NASA requirements for security configuration baselines on all JPL-managed system components and, if necessary, document deviations through a formal risk acceptance process or waivers.

**Management's Response:** Concur. The NASA CIO will work, in conjunction with the Deputy Associate Administrator for SCaN, the NMO, and the JPL CIO, to ensure that IT security configurations are documented, published, consumed, and measured to meet mutually agreed-upon risk management frameworks\ tolerances.

**Estimated Completion Date:** Expected completion date for this activity is February 12, 2016, contingent on analysis of the contract and availability of resources.

**Recommendation 7:** Take steps to ensure the NASA Security Operations Center (SOC) has appropriate oversight at JPL to support NASA's Agency-wide incident management program.

**Management's Response:** Concur. The NASA CIO will validate the current state and work in conjunction with the Deputy Associate Administrator for SCaN, the NMO, and the JPL CIO to ensure that the NASA SOC and JPL SOC are meeting agreed-upon requirements. We will work in conjunction with the Deputy Associate Administrator for SCaN, the NMO, and the JPL CIO to validate the controls and reports that underpin the information sharing processes supporting NASA's incident management program.

**Estimated Completion Date:** Expected completion date for this activity is February 26, 2016, contingent on analysis of the contract and availability of resources.

In order to ensure the physical security requirements for NASA Critical Infrastructure (NCI) are implemented consistently across the DSN Complexes, the OIG recommends the Assistant Administrator for Protective Services in conjunction with the Contracting Officer:

**Recommendation 8:** Review and update the contracts with Canberra and Madrid to include physical security requirements for NCI as stated in NASA policies.

**Management's Response:** Concur. After an accurate Facility Security Level (FSL) has been determined at each of the DSN complexes, the Assistant Administrator for Protective Services, as the Agency Risk Acceptance Authority (RAA) for all NASA security program risks, will coordinate with the Human Exploration and Operations Mission Directorate (HEOMD) on identifying acceptable risks. This will allow for a more direct review of the Canberra and Madrid contracts and identify the necessary modifications to the NMO. It is for this reason that the management action associated with Recommendation 9 must be completed **prior** to undertaking Recommendation 8.

**Estimated Completion Date:** Following completion of Recommendation 9 (estimated to be February 28, 2016). Estimate that contract reviews and modifications will be completed by July 31, 2016.

**Recommendation 9:** Perform facility security assessments in accordance with NASA policy and identify the appropriate Facility Service Level (FSL) for NCI facilities at Goldstone, Madrid, and Canberra and document deviations from NASA policy using the formal risk acceptance process or waivers to requirements by the Assistant Administrator for Protective Services.

**Management's Response:** Concur. In order to accurately identify the FSL, JPL must perform facility security assessments at the Goldstone, Madrid, and Canberra facilities using the criteria specified in NPR 1620.2A (Facility Security Assessments) and NPR 1620.3A (Physical Security Requirements for NASA Facilities and Property). The Office of Protective Services (OPS) will work with NMO/JPL to establish a timeline for the assessments to be completed.

Once JPL has completed the assessments, determined the FSLs, and made applicable recommendations regarding compensatory measures, OPS will analyze the data for security deficiencies. Findings will then be reviewed in order that a determination can be made regarding the level of risk that the Associate Administrator for HEOMD, as the risk acceptance authority for Space Communications and Navigation (SCaN), and the Assistant Administrator for Protective Services, as the Agency RAA for all NASA security programs, are willing to accept. This will then determine if waivers to NASA security policy will be necessary for OPS approval.

**Estimated Completion Date:** OPS will work with NMO/JPL to establish a timeline for the security assessments at Goldstone, Madrid, and Canberra complexes to be completed. Estimate that assessments can be completed and documentation for deviations from NASA policy or waivers to requirements will be finalized by February 28, 2016.

Due to the dynamic nature of technology and a constantly changing threat landscape, the OIG recommends the CIO and Assistant Administrator for Protective Services in conjunction with the NASA Chief Information Security Officer and Contracting Officer:

**Recommendation 10:** Develop a strategy for implementing evolving Federal IT and physical security policies at JPL through means that minimize time-consuming negotiation of formal contract modifications.

**Management's Response: Concur.** The NASA CIO will work, in conjunction with the Deputy Associate Administrator for SCaN, the NMO, the OPS, and the JPL CIO to validate and, where needed, enhance processes and procedures to accommodate three conditions necessary to realize effective cybersecurity that is consistently implemented across NASA and JPL:

(1) Organization Direction. This includes organizational mechanisms for establishing and communicating priorities and objectives, principles, policies, standards, and performance measures.

(2) A Culture of Accountability. This includes aligning internal processes, maintaining accountability, and informing, making, and following through on decisions with implications for cyberspace protection and defense.

(3) Insight and Oversight. This includes measuring, reviewing, verifying, monitoring, facilitating, and remediating to ensure coordinated and consistent cybersecurity implementation and reporting across our organizations without impeding local missions.

The Office of Protective Services will work with the Office of Procurement and the NASA Management Office to ensure that evolving Federal physical and security policies are implemented at JPL in the most expeditious manner possible.

**Estimated Completion Date:** Expected completion date related to IT security policies is March 11, 2016, contingent on analysis of the contract and availability of available resources. Expected completion date related to physical security policies is July 31, 2016.

In order to improve NASA's oversight for the allocable, allowable, and reasonable costs on the DSN foreign contracts, the OIG recommends the Deputy Associate Administrator for SCaN in conjunction with the Contracting Officer:

**Recommendation 11:** Require Instituto Nacional de Técnica Aerospacial (INTA's) representative to submit the required detailed monthly financial status reports.

**Management's Response:** Concur. Immediate delivery of electronic versions has been requested allowing for timely Contracting Officer review and analysis.

**Estimated Completion Date:** Completed. Electronic versions of INTA monthly financial status reports have been requested.

**Recommendation 12:** Request the Defense Contract Audit Agency (DCAA) perform incurred cost audits on the Canberra and Madrid contracts, and if DCAA cannot perform the audits in a timely manner, seek an alternative contract audit service.

**Management's Response:** Concur. DCAA audit requests have been initiated with DCAA for review of incurred costs of the Canberra Deep Space Communication Complex. Although DCAA review of incurred costs for the Madrid Deep Space Communication Complex have been limited recently, due to risk analysis, Contracting Office cost analysis will be performed with support from subject matter experts both within NASA and external sources (e.g. DCMA). Contracting Officer cost analysis will be emphasized and supported with additional training.

**Estimated Completion Date:** Completed. Requests for DCAA incurred cost audits on the Canberra and Madrid contracts have been made.

We have reviewed the draft report for information that we believe should not be publicly released. We have not communicated any concerns regarding the public release of information contained in your report.

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 John Bosco (Audit Liaison Representative/OCIO) at 202-358-1352 or Michelle Bascoe (Audit Liaison Representative/HEOMD) at 202-358-1574.

William H. Gerstenmaier

Larry N. Sweet

cc:
Associate Administrator for Mission Support/ Mr. Keegan
Deputy Associate Administrator for Space Communications and Navigation Program/ Mr. Younes
Assistant Administrator for Protective Services/ Mr. Mahaley
Assistant Administrator for Procurement/ Mr. McNally
Director NASA Management Office/ Mr. Watkins
Director Jet Propulsion Laboratory/ Mr. Elachi

# APPENDIX C: REPORT DISTRIBUTION

## National Aeronautics and Space Administration

Administrator
Associate Administrator
Chief of Staff
Chief Information Officer
Chief Information Security Officer
Associate Administrator, Human Exploration and Operations
    Deputy Associate Administrator, Space Communications and Navigation Program
Associate Administrator, Mission Support
Assistant Administrator, Procurement
Assistant Administrator, Protective Services
Director, NASA Management Office
Director, Jet Propulsion Laboratory

## 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 Competiveness

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-14-012-00)**