NASA

National Aeronautics and Space Administration

Office of Inspector General

Office of Audits

CYBERSECURITY MANAGEMENT AND OVERSIGHT AT THE JET PROPULSION LABORATORY

June 18, 2019

Report No. IG-19-022

Office of Inspector General

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

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

NASA Office of Inspector General
Office of Audits

RESULTS IN BRIEF

Cybersecurity Management and Oversight at the Jet Propulsion Laboratory

June 18, 2019 IG-19-022 (A-18-012-00)

WHY WE PERFORMED THIS AUDIT

NASA's Jet Propulsion Laboratory (JPL) is a federally funded research and development center in Pasadena, California. Since 1959, the California Institute of Technology (Caltech) has been under contract with NASA to manage JPL, most prominently its research and development activities, but also its network security controls. Under the contract, NASA retains responsibility for ensuring Agency data and systems at JPL are secure from hackers or other forms of unauthorized access.

JPL's information technology (IT) systems maintain a wide public internet presence while supporting missions and networks that control spacecraft, collect and process scientific data, and perform critical operations. Over the past 10 years, JPL has experienced several notable cybersecurity incidents that have compromised major segments of its IT network. For example, in 2011 cyber intruders gained full access to 18 servers supporting key JPL missions and stole 87 gigabytes of data. More recently, in April 2018 JPL discovered an account belonging to an external user had been compromised and used to steal approximately 500 megabytes of data from one of its major mission systems.

In this audit, we assessed the effectiveness of JPL's network security controls for externally facing applications and systems. We also examined elements of JPL's Cybersecurity Program and NASA's interaction with and oversight of the IT security control responsibilities assigned to Caltech under its contract to manage JPL. To complete this work, we interviewed NASA and JPL IT officials and reviewed JPL's IT network mapping, system inventory, and security management tools. We also reviewed federal, NASA, JPL, and Caltech criteria, policies, procedures, supporting documentation, agreements, prior audit reports, external reviews, and other documents related to cybersecurity.

WHAT WE FOUND

Multiple IT security control weaknesses reduce JPL's ability to prevent, detect, and mitigate attacks targeting its systems and networks, thereby exposing NASA systems and data to exploitation by cyber criminals. JPL uses its Information Technology Security Database (ITSDB) to track and manage physical assets and applications on its network; however, we found the database inventory incomplete and inaccurate, placing at risk JPL's ability to effectively monitor, report, and respond to security incidents. Moreover, reduced visibility into devices connected to its networks hinders JPL's ability to properly secure those networks. Further, we found that JPL's network gateway that controls partner access to a shared IT environment for specific missions and data had not been properly segmented to limit users only to those systems and applications for which they had approved access. This shortcoming enabled an attacker to gain unauthorized access to JPL's mission network through a compromised external user system. Additionally, NASA failed to establish Interconnection Security Agreements (ISA) to document the requirements partners must meet to connect to NASA's IT systems and describe the security controls that will be used to protect the systems and data.

We also found that security problem log tickets, created in the ITSDB when a potential or actual IT system security vulnerability is identified, were not resolved for extended periods of time—sometimes longer than 180 days. While system administrators may request a waiver when they cannot resolve such tickets within 6 months, we found waivers were not reviewed annually as required, resulting in unnecessary waivers and potentially outdated compensating

security controls that expose the JPL network to exploitation by cyberattacks. Further, JPL system administrators misunderstood their responsibilities regarding management and review of logs for identifying malicious activity occurring on a particular system or network. We also found that while cybersecurity monitoring tools employed by JPL defend against routine intrusions and misuse of computer assets, JPL had not implemented a threat hunting program recommended by IT security experts to aggressively pursue abnormal activity on its systems for signs of compromise, and instead rely on an ad hoc process to search for intruders. In addition, JPL had not provided role-based security training or funded IT security certifications for its system administrators.

Further, we found that multiple JPL incident management and response practices deviate from NASA and recommended industry practices. For example, unlike NASA's Security Operations Center (SOC), JPL's SOC does not maintain round-the-clock availability of IT security incident responders and JPL's incident response plan does not include all federally-recommended elements. In addition, team coordination issues delayed completion of incident containment and eradication steps for the April 2018 incident. Moreover, while documenting and sharing cyber threat information across JPL to help prevent future incidents is a critical component of an effective incident response program, we found JPL's current initiatives fall short.

Finally, while the contract between NASA and Caltech requires JPL to report certain types of IT security incidents to the Agency through the NASA SOC incident management system, no controls were in place to ensure JPL compliance with this requirement nor did NASA officials have access to JPL's incident management system. Collectively, these weaknesses leave NASA data and systems at risk.

Despite these significant concerns, the contract NASA signed with Caltech in October 2018 to manage JPL for at least the next 5 years left important IT security requirements unresolved and instead both sides agreed to continue negotiating these issues. As of March 2019, the Agency had not approved JPL's plans to implement new IT security policies and requirements NASA included in its October 2018 contract.

WHAT WE RECOMMENDED

To improve JPL network security controls, we recommended the Director of the NASA Management Office instruct the JPL Chief Information Officer (CIO) to: (1) require system administrators to review and update the ITSDB and ensure system components are properly registered and the JPL Cybersecurity/Identity Technologies and Operations Group (CITO) periodically review compliance with this requirement; (2) segregate shared environments connected to the network gateway and monitor partners accessing the JPL network; (3) review and update ISAs for all partners connected to the gateway; (4) require the JPL CITO to identify and remediate weaknesses in the security problem log ticket process and provide periodic aging reports to the JPL CIO; (5) require the JPL CITO to validate, update, and perform annual reviews of all open waivers; (6) clarify the division of responsibility between the JPL Office of the Chief Information Officer and system administrators for conducting routine log reviews and monitor compliance on a more frequent basis; (7) implement the planned role-based training program by July 2019; (8) establish a formal, documented threat-hunting process; and (9) develop and implement a comprehensive strategy for institutional IT knowledge and incident management that includes dissemination of lessons learned. We also recommended the NASA CIO include requirements in the pending IT Transition Plan that provide the NASA SOC with sufficient control and visibility into JPL network security practices.

We provided a draft of this report to NASA management who concurred with 9 of our 10 recommendations and described corrective actions it has taken or will take. We consider management's comments to those recommendations responsive and therefore the recommendations are resolved and will be closed upon completion and verification of the proposed corrective actions. Management did not concur with Recommendation 8 related to establishing a cybersecurity threat-hunting capability and this recommendation will remain unresolved pending further discussion with the Agency.

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

ASR	Application Security Registry
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CITO	Cybersecurity/Identity Technologies and Operations Group
DHS	Department of Homeland Security
DSN	Deep Space Network
GAO	Government Accountability Office
HMM	Hunting Maturity Model
IP	Internet Protocol
ISA	Interconnection Security Agreement
IT	information technology
ITSDB	Information Technology Security Database
JPL	Jet Propulsion Laboratory
JPL SOC	Jet Propulsion Laboratory Cybersecurity Operations Center
NIST	National Institute of Standards and Technology
NPD	NASA Policy Directive
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
SAISO	Senior Agency Information Security Officer
SOC	Security Operations Center
SP	Special Publication
SPL	security problem log
US-CERT	United States Computer Emergency Readiness Team

INTRODUCTION

Cyberattackers seek to gain unauthorized access to a target's information systems to steal sensitive data, disrupt an organization's critical operations, pursue political or financial objectives, or merely to test their hacking skills. These bad actors include individuals, hacking organizations, criminal groups, and foreign governments. As one of the leading governmental science and technology agencies in the world, NASA is an attractive target with Agency operations and sensitive data related to International Traffic in Arms Regulations, intellectual property, personally identifiable information, and safety-related flight system data at risk.[1] Potential infiltration into NASA's space flight systems to acquire launch codes and flight trajectories of spacecraft remains a particular concern of NASA information technology (IT) security managers. The Agency's IT security controls face added challenges because of NASA's extensive connectivity with its many external users and partners, including foreign space agencies, commercial contractors, and educational institutions. Moreover, the use of legacy IT systems for long-standing missions that may have been launched decades ago further complicate NASA's security challenges because of outdated and unpatched software and operating systems.

In addition to its nine geographically dispersed Centers, NASA has a contract with the California Institute of Technology (Caltech), a private nonprofit research university, to operate the Jet Propulsion Laboratory (JPL) in Pasadena, California, as a federally funded research and development center.[2] JPL manages or supports multiple deep space missions for NASA such as the Mars Science Laboratory and Juno.[3] Since 1959, Caltech has managed JPL's research and development activities, including security controls over its data and systems. Nevertheless, NASA retains responsibility for ensuring its data and systems at JPL and the other Centers are secure from hackers or other forms of unauthorized access.

Over the past 10 years, JPL has experienced several cybersecurity incidents that have compromised its IT network. For example, in February 2012 the NASA Inspector General testified before Congress about multiple sophisticated attacks on JPL's network that allowed intruders full access to key JPL systems and sensitive user accounts.[4] More recently, in April 2018 JPL discovered that an account belonging to an external user had been compromised and used to access one of its major mission systems.

---

[1] International Traffic in Arms Regulations control the transfer of military and space-related technology. Under these federal regulations, foreign nationals are not permitted access to such export-controlled information unless they receive a license from the U.S. Department of State. Intellectual property involves patents or other forms of protection to safeguard the government's rights to ideas, inventions, and technologies to which NASA holds title. Personally identifiable information is any information about an individual maintained by an agency that can be used to distinguish or trace their identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records and information linked to an individual such as medical, educational, financial, and employment information.

[2] The NASA Management Office manages the Agency's contract with Caltech for operation of JPL, provides NASA Headquarters with on-site Agency oversight of contractor activities, and ensures regulatory compliance of contractor operations.

[3] The Mars Science Laboratory is NASA's latest rover mission to the Red Planet and has been operating on its surface since August 2012. The Juno mission, which began orbiting Jupiter in July 2016, is designed to improve NASA's understanding of Jupiter's origins and evolution by mapping the planet's gravity and magnetic fields and observing the composition of its atmosphere.

[4] NASA Cybersecurity: An Examination of the Agency's Information Security. Before the Subcommittee on Investigations and Oversight, House Committee on Science, Space, and Technology, 112th Congress (2012).

Given the criticality of JPL's mission and the differing relationship NASA has with JPL in establishing IT security controls compared to other Centers, we initiated this audit to assess the effectiveness of JPL's network security controls for externally facing applications and systems. In addition, we examined elements of JPL's Cybersecurity Program and NASA's interaction with and oversight of the IT security control responsibilities assigned to Caltech under its contract to manage JPL. See Appendix A for details on our scope and methodology.

Background

NASA's mission IT network is distributed throughout the United States and hosts hundreds of systems and projects. The Agency's IT portfolio includes systems that control spacecraft, collect and process scientific data, provide security for critical infrastructure, and enable Agency personnel to collaborate with colleagues around the world. Although most of these systems contain data appropriate for wide dissemination, some contain sensitive information that, if stolen or inappropriately released, could result in significant financial loss, jeopardize mission safety, or adversely affect national security. Further, NASA maintains a substantial internet presence, sharing information on its aeronautics, science, and space programs with the public and research community through thousands of publicly accessible web applications.[5] In addition, NASA has numerous web portals and applications that enable Agency civil servants and contractors to access data and services remotely from around the world.

Threats to federal information systems have grown and evolved over the years, including the sophistication and effectiveness of cyberattacks. Since 1997 the Government Accountability Office (GAO) has designated federal information security as a government-wide high-risk area that requires focused attention. Indeed, the number of information security incidents reported by federal agencies increased from 5,503 in fiscal year 2006 to 77,183 in fiscal year 2015—an increase of 1,303 percent.[6] While adversaries of varying capabilities and motivations have utilized diverse techniques to take advantage of security vulnerabilities, federal networks and systems are targeted by persistent, sophisticated attacks—commonly known as advanced persistent threats—operating on behalf of nation states or organized criminal groups who often have the ability to maintain long-term access to targeted networks. The extensive planning and dedicated efforts behind advanced persistent threats increase their chances of success and reduce the ability of organizations to detect their presence in a timely manner. In addition, adversaries are often effective at stealing legitimate user credentials through social engineering techniques to gain access to targeted networks.[7]

Not surprisingly, NASA is a regular target of cyberattacks both because of the large size of its networks and the sensitive nature of the information it maintains. The Agency's substantial connectivity with nongovernmental educational and research institutions also presents cyber criminals with a larger, more attractive target than most other government agencies and offers cyberattackers multiple points of entry into the Agency's various networks. Accessing NASA's research and development on Earth science and advanced space technologies remain a priority for hostile foreign nations seeking to gain a

[5] As of December 2018, the Agency's internet footprint included 3,046 public websites.

[6] GAO, *Federal Information Security: Weaknesses Continue to Indicate Need for Effective Implementation of Policies and Practices* (GAO-17-549, September 28, 2017).

[7] Social engineering attacks employ human interaction (social skills) to obtain or compromise information about an organization or its computer systems. A common form of social engineering is phishing, which uses email or malicious websites to solicit personal information by posing as a trustworthy individual or organization.

competitive economic or military advantage. Bad actors routinely leverage publicly available open source information to develop attack paths and techniques targeting NASA information, including space-based robotics, data acquisition systems, and aeronautic systems technology for unmanned aerial vehicles and fighter aircraft.

With IT security threats at NASA increasing in number and complexity, detecting and promptly responding to these threats has become an essential part of the Agency's IT security program. Effective cybersecurity for information systems remains critical to preventing the compromise of sensitive information, disruption of mission operations, and damage to the Agency's reputation due to embarrassing cyber incidents. In addition to multiple IT-related reports we have issued over the past 10 years, a recent GAO report found NASA ineffective in implementing leading IT management practices in strategic planning, workforce planning, governance, and cybersecurity.[8]

NASA and JPL IT Security Organizational Structures

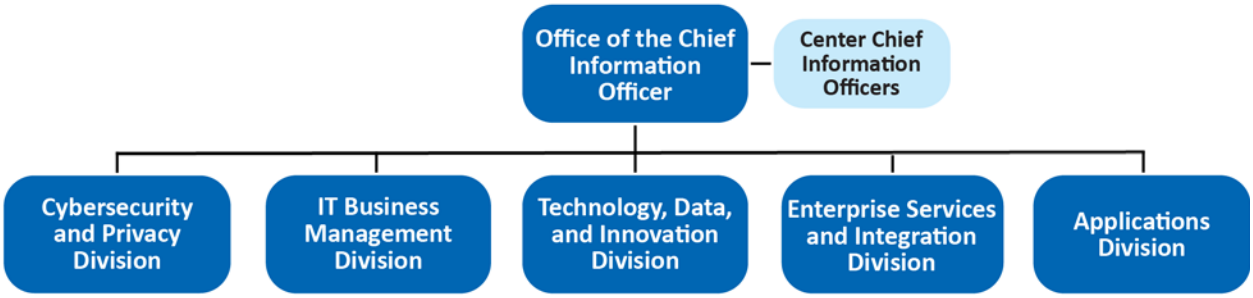
NASA IT Organizational Structure

NASA's Office of the Chief Information Officer (OCIO) is responsible for the Agency's IT governance as well as managing and securing its IT systems, assets, and operations. In addition to the Headquarters-based Agency Chief Information Officer (CIO) and OCIO staff, each NASA Center, including JPL, has a CIO and dedicated IT staff. The Federal Information Security Management Act of 2002 directs the CIO for each agency to identify a Senior Agency Information Security Officer (SAISO), also known as an agency Chief Information Security Officer (CISO). The SAISO is the principal advisor to the Agency CIO and other senior officials on matters pertaining to information security. JPL's CISO does not report directly to the NASA SAISO, instead reporting to the JPL CIO, but coordinates with the SAISO on Agency-wide IT matters and cybersecurity incidents.

The Headquarters OCIO is organized into five divisions, including a Cybersecurity and Privacy Division that manages Agency-wide security projects to correct known system vulnerabilities and provide IT security services in support of NASA's information systems. Figure 1 illustrates the OCIO organizational structure as of April 2019. As part of these cybersecurity efforts, NASA operates a Security Operations Center (SOC) located at Ames Research Center as its central coordination point for continuous monitoring of computer network traffic entering and leaving NASA facilities. The NASA SOC operates the Incident Management System that coordinates, tracks, and reports on IT security incidents across the Agency.

[8] GAO, *NASA Information Technology: Urgent Action Needed to Address Significant Management and Cybersecurity Weaknesses* (GAO-18-337, May 22, 2018).

Figure 1: NASA OCIO



Source: NASA Office of Inspector General (OIG) presentation of NASA Policy Directive 1000.3E, *The NASA Organization w/Change 39 (approved October 26, 2018)*, April 15, 2015, information.

JPL IT Organizational Structure

NASA's contract with Caltech covers all research and development activities as well as management and institutional operation of JPL, including IT services. Through its contract, NASA shares authority and responsibility with Caltech for developing IT policies and implementing an IT security program to protect the Agency's assets and respond to security incidents. Specifically, the contract requires that JPL establish and maintain procedures to "substantiate that JPL-related IT and information resources are acquired and managed in a manner that safeguards NASA's IT infrastructure, systems, assets, and information." As NASA's OCIO management described the relationship, the Agency establishes the level of security and controls required to operate JPL, but allows Caltech flexibility to decide how to achieve those requirements. As such, Caltech selects and implements IT security controls, including incident monitoring and handling controls, to protect the confidentiality, integrity, and availability of NASA electronic information from unauthorized disclosure.

JPL's IT directorate, known as the JPL OCIO, provides IT services to support NASA missions carried out by JPL. JPL also operates its own incident response team out of the JPL Cybersecurity Operations Center (JPL SOC). Led by the Cybersecurity/Identity Technologies and Operations Group (CITO), the JPL SOC provides support in application and vulnerability assessments, log data analysis, and cybersecurity monitoring and investigations.[9] The JPL SOC includes technical investigators who gather information relevant to understanding the scope and location of an incident and forensic analysts who assess the collected information and generate reports based on their findings. These teams often collaborate during incident investigations and work with JPL system administrators or network operators to strategize incident containment, eradication, and remediation tasks. From a governance perspective, JPL's CIO retains approval authority for cybersecurity incident response while JPL's CISO coordinates multi-division resources for incident handling and remediation efforts.

[9] CITO's responsibilities include cybersecurity risk management, monitoring and detection, threat analysis, vulnerability identification, specification of required corrective actions, requirements, protective measures and automated support for security planning and risk acceptance, incident investigations, training and awareness curriculum and newsletters, and engineering support for institutional IT security services.

NASA SOC and JPL SOC have agreed in principle to a set of cybersecurity event and incident reporting requirements for each organization in a Service Levels Objectives agreement.[10] Specifically, the JPL SOC reports all JPL-related IT security events and incident data originating on networks that JPL manages based on the agreed-upon event types, including data exposure, unauthorized access, and denial of service incidents.[11] The JPL SOC must also provide the NASA SOC with indicators of compromise and warnings gathered by security assessment and monitoring tools used to identify and investigate cybersecurity incidents within the JPL environment when the compromise has the potential to impact other NASA Centers' operations or missions (e.g., due to interconnectivity through shared mission networks). Similarly, the NASA SOC provides information to assist in analyzing and resolving incidents when JPL systems could be impacted.

On October 1, 2018, NASA entered into a $15 billion, 5-year contract with Caltech to operate JPL on NASA's behalf. Among the provisions in the contract were several new IT security requirements.[12] However, Caltech's execution of several IT security responsibilities were not agreed upon when the contract was signed, but rather left for further negotiation. Specifically, the new contract stipulates JPL shall provide NASA with an "IT Transition Plan" that reflects Caltech's plan for operations and compliance with its new contractual obligations, including an implementation plan for meeting the intent of the Agency's IT security policies and procedures. However, as of March 2019 the Agency had not approved Caltech's proposed transition and implementation plans.

National Institute of Standards and Technology IT Security Framework

To protect an organization's data, applications, and systems, industry standards and federal regulations recommend implementation of IT standard security controls and processes. The National Institute of Standards and Technology (NIST) developed a comprehensive structure, known as the Framework for Improving Critical Infrastructure Cybersecurity, to assist agencies in managing cybersecurity risks and ensuring the effectiveness of security controls over information resources. The framework focuses on five specific functions essential to an effective information security program:

1. *Identify* a network's components including an inventory of physical assets, connectivity, and resources that support it.
2. *Protect* the network by preventing unapproved access by unauthorized users to its applications and systems.
3. *Detect* vulnerabilities that can be exploited by unauthorized users were they to gain access to the network, intrusions by unauthorized users who seek to exploit vulnerabilities in a network, and configuration and coding changes executed by unauthorized users.

[10] Despite operating under the requirements established in the agreement, as of March 2019 NASA and Caltech had not signed a final version of the agreement.

[11] A denial of service event is an attack that successfully prevents or impairs the normal functionality of networks, systems, or applications by exhausting resources.

[12] The cost-plus-fixed-fee, indefinite-delivery, indefinite-quantity contract has a maximum value of $30 billion and seeks to hold JPL IT systems to the same cybersecurity standards in place at other NASA Centers, including federally mandated requirements in the Federal Information Security Modernization Act of 2014 and Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources* (February 8, 1996).

4. *Respond* timely and effectively to intrusions to stop and contain the exploit in a manner that is commensurate with the level of threat it represents.[13]
5. *Recover* systems and applications impacted by attacks, including communication of incidents and reconfiguration of the network to prevent repeat attacks.

Together, these functions provide a strategic view of the life cycle of an organization's cybersecurity risk management program and ensure the security controls in place protect the confidentiality, integrity, and availability of an organization's data, applications, and systems.

JPL IT Security Processes

IT Network Architecture and System Categorization

As of December 3, 2018, JPL's IT network was comprised of 26,714 computer systems that includes 3,511 servers.[14] Similar to NASA, JPL's IT assets generally fall into two broad categories: institutional and mission. Institutional systems support the day-to-day work of JPL employees and include desktop and laptop computers, end-user tools such as email and calendaring, and data centers to provide hosting, storage, and computing capabilities. Mission systems support JPL's space exploration programs and host IT systems that control spacecraft such as the Voyager missions and Mars rovers, and collect and process scientific data (see Appendix B for a description of the JPL mission support areas).

From a high-level perspective, the JPL network contains three subnetworks: a network that supports administrative and support operations; a network that supports NASA missions currently in operation or development (see Appendix B); and a network that supports the Deep Space Network (DSN), which JPL operates on behalf of NASA.[15] To control access and protect systems connected to these subnetworks, JPL has established multiple firewalls.[16] NASA Centers and external partners, such as foreign space agencies and educational institutions, access the DSN and communicate with JPL mission systems through a remote network gateway.[17] To monitor and control access between systems and applications, in March 2017 JPL began implementing a zone-based architecture to provide an additional layer of security and segregation of critical systems within the subnetworks and limit indirect access through external facing applications.

---

[13] An exploit is an attack on a computer system, especially one that takes advantage of a particular vulnerability such as a weakness in an operating system, application, or software code.

[14] These numbers fluctuate over time. A server is a computer, device, or program dedicated to managing network resources.

[15] The DSN—the largest and most sensitive scientific telecommunications system in the world—is NASA's international array of giant radio antennas that support interplanetary spacecraft missions as well as a few that orbit Earth. Consisting of facilities located in Goldstone, California; near Madrid, Spain; and near Canberra, Australia, the DSN provides the crucial connection for commanding our spacecraft beyond Earth and receiving their data and scientific information.

[16] A firewall is an inter-network connection device that restricts data communication traffic between two connected networks. A firewall may be either an application installed on a general-purpose computer or a dedicated platform (appliance) that forwards, rejects, or drops data packets on a network.

[17] Foreign partners include France's Centre National d'Etudes Spatiales, European Space Agency's European Space Operations Centre in Germany, Indian Space Research Organisation, and Japan Aerospace Exploration Agency. A gateway is a node (often associated with a router) in a computer network, a key stopping point for data on its way to or from other networks. A router is a computer or network-related hardware that connects to the internet.

Vulnerability Detection and Remediation

JPL security requirements for access control and system flaw remediation specify that patch management software be installed on all computers and configured to report patch status, and that successful and failed log in and log off efforts be recorded in system and application log files.[18]

Additionally, JPL system administrators are required to review system log files regularly for suspicious or unusual activity. JPL's CITO uses vulnerability scans to assess the security posture of network-enabled systems through automated analysis of open network ports and services while examining system patch levels.[19] Externally facing systems are regularly scanned and the entire JPL network is scanned at least monthly. When CITO identifies a vulnerability, a security problem log (SPL) ticket is issued and the system administrator must take corrective action to address the problem. The SPL ticket identifies the security violation and includes a description of the problem with a recommended corrective action. System administrators commonly remediate vulnerabilities by applying a software patch, updating a system's configuration, or adding a compensating control such as encryption to ensure data integrity. A CITO analyst will verify that corrective actions taken by the system administrator satisfactorily address the problem listed in the SPL ticket before closing it. System administrators may request a waiver or lien when a ticket cannot be remediated within the specified timeframe.[20]

Incident Management and Response

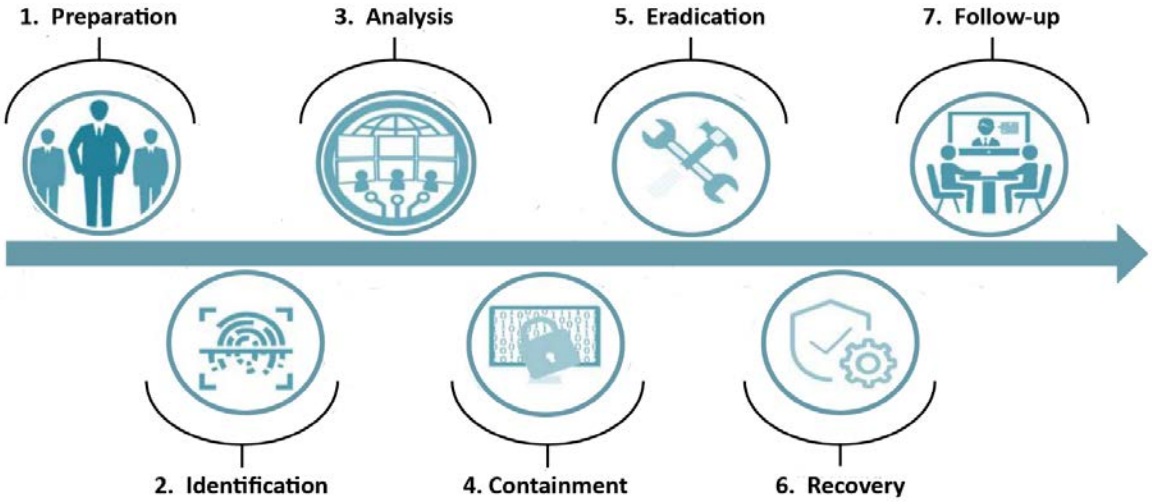
Given the persistence of bad actors and the constant evolution of hacking tools, the IT security industry emphasizes timely detection and effective response to cybersecurity incidents. Accordingly, JPL has developed a Cybersecurity Incident Response Plan detailing the roles, responsibilities, and processes for responding to cyber-related incidents impacting JPL. In general, JPL follows the incident management and response life cycle adopted by the NASA SOC, which adheres to guidelines published by NIST. The process, depicted in Figure 2, includes seven phases—preparation, identification, analysis, containment, eradication, recovery, and follow-up.

[18] A patch is an update to an operating system, application, or other software issued to correct particular problems with the software. Patch management software supports the systematic notification, identification, deployment, installation, and verification of operating system and application patches.

[19] Vulnerability scanners are specialized commercial software programs that automate the vulnerability detection process. These programs search databases for known vulnerabilities associated with commonly used computer operating systems and software applications. When a match is found, the scanner alerts the operator to a possible vulnerability. The scanners rank vulnerabilities according to their potential to harm the system, allowing organizations to prioritize and address their most critical vulnerabilities.

[20] A waiver is an open-ended request for permission to forego correcting the vulnerability or implementing a requirement. A lien is a request to delay implementation of a new requirement or the correction of a vulnerability. A lien must include a specific date the delay will end. Waivers and liens must be approved by the IT Security Group Manager, Line Manager, Division Manager (or Director), and the JPL CISO.

Figure 2: Incident Response Phases



Source: NASA OIG presentation of information from NASA IT Security Handbook 2810.09-02A, *NASA Information Security Incident Management Handbook*, March 17, 2017.

When an IT security event or incident is suspected, JPL activates an incident response team to conduct an investigation, implement containment and eradication strategies, and coordinate incident response with the NASA SOC, if necessary. Security events can be identified from a variety of sources, including intrusion detection systems, JPL users, the NASA SOC, and other external entities.[21] JPL's SOC provides continuous monitoring and event detection through a combination of manual and automated tools, dashboards, and alert systems.[22] If an event is determined to be a valid incident, an investigator opens a ticket in JPL's Incident Management System to document, report, and track the progress of the investigation. The investigator and JPL SOC Group Lead and Group Supervisor work collaboratively to eliminate the threat from the environment, restore affected systems to normal operational status, and implement additional security monitoring or controls to prevent future incidents.

Notable External Attacks of the JPL Network

The threat to JPL's computer networks from internet-based intrusions is real and expanding in scope and frequency.

- In January 2009, a cyberattacker successfully penetrated a computer system at JPL and extracted approximately 22 gigabytes of program data by illegally transferring the information to an Internet Protocol (IP) address in China. The stolen data included information protected under International Traffic in Arms Regulations and Export Administration Regulations.[23] A follow-on NASA Office of Inspector General (OIG) investigation found that a significant

[21] An intrusion detection system is software that automates the intrusion detection process and is used by organizations to support their incident response efforts. It can monitor and analyze events to identify undesirable activity, provide alerts to security administrators, and record information related to observed events.

[22] Dashboards present and communicate data in an organized, visual format for users to interpret and monitor activity on their systems or within their networks.

[23] Export Administration Regulations regulate the export of "dual-use" items, including goods and related technology such as computers and aircraft, which possess both commercial and military applications.

contributing factor to the theft was inadequate security settings across various network points, including several computers and a server at JPL, which allowed the intruder to access a wide range of sensitive data. To mitigate future attacks, JPL deployed host-based firewalls and intrusion prevention systems on workstations and implemented network segmentation throughout the JPL network to limit the spread of malware.[24]

- In 2011, JPL discovered another attack involving Chinese-based IP addresses in which cyber intruders gained full access to 18 servers supporting key JPL missions, including the DSN and Advanced Spaceborne Thermal Emission and Reflection Radiometer mission, and sensitive user accounts.[25] With full system access, the intruders were able to: (1) copy, modify, or delete sensitive files; (2) add, modify, or delete user accounts for mission-critical JPL systems; (3) upload hacking tools to steal user credentials and compromise other NASA systems; and (4) modify system logs to conceal their actions. Intruders resided within the system for 2 weeks before being detected and analysis of intrusion detection system log files revealed 87 gigabytes of data had been uploaded to the attackers' IP addresses. In response to this intrusion, JPL implemented automated means for identifying malicious activity and placed JPL SOC personnel on call to respond to such breaches.
- In 2014, JPL discovered a cyber intruder was able to upload malware to a server supporting JPL astronomical missions and research after a web-based program installed by the system's administrator allowed the public to upload and execute files on the server. Investigation of the compromise revealed the administrator failed to update the software in a timely manner, providing the attacker an opportunity for unauthorized access via a JPL computer. JPL OCIO responded by applying additional network controls, including intrusion prevention systems and further network segmentation, to prevent public-facing servers from accessing the internal JPL network.
- In 2016, a website misconfiguration resulted in an anonymous user gaining elevated privileges that enabled an individual to execute codes on a server used for software architecture development. The use of Secure Sockets Layer, which ensures that all data transmitted between the web server and browser remains encrypted, prevented JPL's network security monitoring tools from identifying the actions taken by the bad actor prior to detection.
- In March 2017, a JPL server that runs source code used in ground operations for scientific spacecraft was compromised by foreign hackers who exploited a flaw in the software, hardware, or firmware that was previously unknown to JPL. As a result, the intruders remotely executed a code on the server without authentication. After gaining access to the server, the hackers were able to upload, manipulate, and execute various files and commands unrelated to controlling spacecraft. Analysis by the OIG determined the system had not been patched on time nor did the system owner timely review the application log to identify suspect activities. Post-incident remediation by the JPL OCIO included routine content filtering at external firewall points and improvements to its software use policy to require prior approval.

[24] Host-based firewalls monitor and control incoming and outgoing network traffic for a single server and provide an additional layer of security beyond the network perimeter. Malware refers to a program that is inserted into a system, often covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system.

[25] Advanced Spaceborne Thermal Emission and Reflection Radiometer, a cooperative effort between NASA and Japan's Ministry of Economy, Trade and Industry, is an Earth observing instrument providing useful data about land surface temperature, vegetation and soil distribution, and hydrology, among other science research and applications.

- In April 2018, JPL discovered an account belonging to an external user used to log into JPL's mission network had been compromised. Given the architecture of JPL's network, the attackers were able to expand their access upon entry and move laterally across the network. Classified as an advanced persistent threat, the attack went undetected for nearly a year. The investigation into this incident is ongoing. In response to the attack, JPL installed additional monitoring agents on its firewalls and continues to work with NASA to review network access agreements for external partners.

Ultimately, the scope and success of these intrusions demonstrate the increasingly complex nature of IT security challenges facing JPL and the Agency. For example, the April 2018 attack on JPL's network illustrates how sophisticated attackers can exploit weaknesses within JPL's system of security controls. Advanced persistent threat attackers patiently and methodically move from system to system searching for weaknesses in a network to advance their attack. In this case the attacker, using an external user account, exploited weaknesses in JPL's system of security controls to move undetected within the JPL network for approximately 10 months. Prior to detection and containment of the incident, the attacker exfiltrated approximately 500 megabytes of data from 23 files, 2 of which contained International Traffic in Arms Regulations information related to the Mars Science Laboratory mission.[26]

More importantly, the attacker successfully accessed two of the three primary JPL networks. Accordingly, NASA questioned the integrity of DSN data related to space flight systems and temporarily disconnected several space flight-related systems from the JPL network.

[26] The Mars Science Laboratory Curiosity Rover is a roving science laboratory designed to collect Martian soil and rock samples, analyze surface radiation, and make detailed measurements of element composition and organic compounds.

WEAKNESSES IN JPL IT SECURITY CONTROLS RISK EXPLOITATION OF NASA SYSTEMS AND LOSS OF DATA

Multiple IT security control weaknesses reduce JPL's ability to effectively prevent, detect, and mitigate attacks targeting its systems and networks and the NASA information on those systems and networks. Specifically, JPL did not have a complete and accurate inventory of all system components on its network, nor did the security controls in place to monitor and detect cyber events and incidents consistently operate as intended. In addition, multiple JPL incident management and response practices such as the staffing of its SOC and the maturity of its operating plans deviated from NASA and recommended industry practices. Taken together, these shortcomings expose Agency systems, data, and applications to exploitation by hackers and cyber criminals.

JPL Lacks Adequate Identification of System Components and Segmentation of Its Network

Incomplete and Inaccurate System Component Inventory

JPL did not have complete and accurate information about the types, location, and value of NASA system components and assets connected to its network. A complete and accurate inventory of all devices connected to a network is critical for an organization to effectively monitor, report, and respond to security incidents in its network. JPL uses a web-based application known as the Information Technology Security Database (ITSDB) to track and manage physical assets and applications on its network. JPL policy requires all network-capable devices be listed in the database. The ITSDB is JPL's authoritative source for hardware and software inventories used to support certification, accreditation, and authorizations of JPL systems; make risk-based decisions; and ensure individual system components receive the appropriate security controls.[27] The Application Security Registry (ASR) within the ITSDB is used to manage applications that are externally accessible and supports critical functions such as project problem reporting and action item tracking. Only IT resources registered in the database and approved by the JPL OCIO are permitted to access JPL's internal network.[28] To add a property item into the ITSDB, a system administrator must request a tag number from a JPL assets representative. The system administrator subsequently must request the property item be imported into the ITSDB before linking it

[27] The ITSDB is an automation tool for the certification and accreditation process, consistent with NIST risk management best practices.

[28] JPL Rules 36852 Rev. 15, *Cybersecurity Requirements* (August 21, 2017).

to a specific IT security plan. This ITSDB update is to be performed weekly. Additionally, JPL policy requires line managers assign new property to system security plans and implement required security controls within 30 days of receipt of the new equipment notification.[29]

Furthermore, the JPL OCIO relies on information from the ASR to communicate security issues to system administrators when devices or applications are affected or at risk. The OCIO also relies on the ASR to ensure applications comply with system requirements and to schedule applications for routine scanning. However, the ITSDB was not consistently updated within JPL's 30-day requirement and the ASR inventory data was not accurate or complete. Consequently, unregistered assets on the network and these unknown systems may fail to receive the patches they need. In addition, inaccurate asset inventory can lead to loss of valuable property and data stored on these assets, undermining the efforts of other critical IT security processes. Moreover, assets attached to the network but not entered in the ITSDB may not be vetted and cleared by JPL security officials. As such, JPL may not be able to effectively monitor, report, and respond to security incidents involving the unknown or unregistered assets across its network.

Based on vulnerability scans performed by the Department of Homeland Security (DHS) in April 2018 and reports of critical systems on the JPL network supplied by Caltech, NASA, and the JPL SOC, we judgmentally selected 13 systems and attempted to trace them to the ITSDB and ASR.[30] Four of the 13 systems were not properly recorded and could not be traced in the ASR database. After we notified JPL OCIO officials, they removed external access for one of the systems that did not meet ASR criteria, created an ASR record for another, and corrected existing ASR information for the remaining two systems.[31]

Moreover, system administrators did not consistently update the inventory system when they added devices to the network. Specifically, we found that 8 of 11 system administrators responsible for managing the 13 systems in our sample maintain a separate inventory spreadsheet of their systems from which they periodically update the information manually in the ITSDB. One system administrator told us he does not regularly enter new devices into the ITSDB as required because the database's updating function sometimes does not work and he later forgets to enter the asset information. Consequently, assets can be added to the network without being properly identified and vetted by security officials. The April 2018 cyberattack exploited this particular weakness when the hacker accessed the JPL network by targeting a Raspberry Pi computer that was not authorized to be attached to the JPL network.[32] The device should not have been permitted on the JPL network without the JPL OCIO's review and approval.

---

[29] Line managers identify IT systems and create system records in the ITSDB; appoint system representatives and system administrators; review and submit IT system accreditation packages to authorizing officials; and assign IT assets, including virtual machines and server-side applications, to security plans within 30 days of receiving a new property.

[30] The vulnerability scan performed by DHS was a routine, quarterly scan undertaken in accordance with DHS Binding Operational Directive 15-01, *Critical Vulnerability Mitigation Requirement for Federal Civilian Executive Branch Departments and Agencies' Internet-Accessible Systems* (May 21, 2015).

[31] In October 2018, JPL developed a plan to address this issue and OCIO officials are expected to implement it by the end of June 2019.

[32] A Raspberry Pi is a credit card-sized computer that plugs into a computer monitor or television, uses a standard keyboard and mouse, and is capable of doing everything a desktop computer can do, from browsing the internet to word-processing and playing games.

Inadequate Segmentation of Network Environment Shared with External Partners

JPL established a network gateway to allow external users and its partners, including foreign space agencies, contractors, and educational institutions, remote access to a shared environment for specific missions and data. However, JPL did not properly segregate individual partner environments to limit users only to those systems and applications for which they had approved access. By properly segmenting a network, an organization creates boundaries an attacker cannot cross by eliminating connections to other systems. As a result, the shared environment lacked appropriate security controls to prevent partners from accessing a variety of exploration and human space flight mission data.[33]

The cyberattacker from the April 2018 incident exploited the JPL network's lack of segmentation to move between various systems connected to the gateway, including multiple JPL mission operations and the DSN. As a result, in May 2018 IT security officials from the Johnson Space Center (Johnson), which handles such programs as the Orion Multi-Purpose Crew Vehicle and International Space Station, elected to temporarily disconnect from the gateway due to security concerns.[34] Johnson officials were concerned the cyberattackers could move laterally from the gateway into their mission systems, potentially gaining access and initiating malicious signals to human space flight missions that use those systems. At the same time, Johnson IT security officials discontinued use of DSN data because they were concerned it could be corrupted and unreliable.

Deep Space Network Dish in Goldstone, California

Source: NASA.

Johnson reestablished its gateway connection in November 2018 and restored use of limited spacecraft data in March 2019. However, as of March 2019, Johnson had not restored its use of all communications data because of continuing concerns about its reliability. While assessing exposure of their network via systems connected to the gateway, Johnson IT security officials also determined they lacked a required security agreement with JPL known as an Interconnection Security Agreement (ISA).[35] NASA's Space Communications and Navigation program is responsible for establishing the ISAs for the connection between Johnson and the DSN. Once established, JPL is responsible for implementation and management of the security agreements. NIST explains that the "ISA is a security document that specifies the technical and security requirements for establishing, operating, and maintaining the interconnection. Specifically, the ISA documents the requirements for connecting the IT systems, describes the security controls that will be used to protect

[33] According to JPL officials, the gateway has since been moved to a different zone in the JPL network that is properly segmented to mitigate unauthorized lateral movement to the mission and institutional networks.

[34] NASA is developing the Orion crew capsule to carry a crew of four astronauts to destinations beyond low Earth orbit on the Agency's new heavy-lift rocket, the Space Launch System.

[35] The ISA was subsequently established in November 2018.

the systems and data, contains a topological drawing of the interconnection, and provides a signature line."[36] The Office of Management and Budget (OMB) requires agencies to obtain written management authorization before connecting their IT systems to other systems, based on an acceptable level of risk. The written authorization should define the rules of behavior and controls that must be maintained for the system interconnection, and it should be included in the organization's system security plan.[37] According to Johnson IT security officials, an up-to-date ISA would have facilitated their decision-making during the attack by identifying the systems and data that might be exposed through their connection to the gateway. Additionally, such an agreement would have provided Johnson officials with the necessary contact information for timely notification of the incident and appropriate coordination for ensuring a well-informed response to their exposure.

Similarly, we found that NASA did not establish an ISA with the external user whose account was compromised in the April 2018 incident and instead JPL used a mission-level agreement—an "Operation Interface Control Document"—that provided the user network access through the remote gateway. According to JPL IT security officials, the mission-level agreement is less detailed and does not contain the same level of security requirements as an ISA. Specifically, it does not (1) document the requirements partners must meet in order to connect to NASA's IT systems, (2) describe the security controls that will be used to protect the systems and data, or (3) contain a topological drawing of the interconnection. As of March 2019, the JPL OCIO was in the process of reviewing a draft ISA for the affected user to replace the mission-level agreement. OCIO officials also noted that they did not have ISAs in place for other external users that access the remote gateway.[38] Without this key information regarding the connecting IT systems and their related security controls, JPL networks remain vulnerable to additional cyberattacks.

Deficiencies in JPL Event Monitoring and Security Controls

Untimely Security Problem Log Ticket Resolution and Patch Application

When a potential or actual IT system security vulnerability is identified, JPL CITO creates a security problem log (SPL) ticket in the ITSDB management system. After an SPL ticket is issued, the system administrator has a maximum of 30 days to take corrective action, depending on the severity of the vulnerability.[39] The ticket identifies the security violation and includes a description of the problem and a recommended corrective action, with system administrators commonly remediating such vulnerabilities by applying a software patch or updating a system's configuration.

[36] NIST Special Publication (SP) 800-47, *Security Guide for Interconnecting Information Technology Systems* (August 2002).

[37] OMB Circular A-130.

[38] As of March 2019, JPL OCIO officials stated they were working with NASA's Senior Agency Information Security Officer to review ISAs with all external partners to ensure access is limited to only required ports, protocols, and data.

[39] JPL Rules 36852 Rev. 15.

We reviewed the 8 system security plans associated with the 13 systems we judgmentally sampled and found significant deficiencies. Specifically, these plans had a total of 5,406 unresolved SPLs—about 86 percent of which were rated high or critical—and four plans contained 666 open SPLs with critical vulnerabilities (see Table 1).[40]

Table 1: Number of Unresolved Critical SPL Tickets

Plan	Number of Unresolved (Open) SPLs	Number of SPLs with a Critical Score of 10
7	5,182	635
160	5	0
154	36	4
149	3	0
257	12	0
265	46	23
574	122	4
593	0	0
Total	**5,406**	**666**

Source: NASA OIG analysis of JPL data.

In addition, five of the plans had a total of 3,137 unresolved SPL tickets open for more than 60 days (see Table 2).

Table 2: Number of Days SPL Tickets Remain Unresolved

Plan	1-30 Days	31-60 Days	61-90 Days	91-180 Days	>180 Days	Total
7	1,069	1,115	2,659	230	109	5,182
160	4	-	-	-	1	5
154	13	3	3	14	3	36
149	3	-	-	-	-	3
257	7	1	2	2	-	12
265	6	5	23	2	10	46
574	34	9	7	14	58	122
593	0	-	-	-	-	0
Total	**1,136**	**1,133**	**2,694**	**262**	**181**	**5,406**

Source: NASA OIG analysis of JPL data.

JPL did not effectively address a known software vulnerability, first identified in 2017, with a critical score of 10. This software flaw can be used by cyberattackers to remotely execute malicious code, encrypt data on a targeted system, and demand payments to unlock the data. From March to April 2018, the JPL OCIO issued 16 SPL tickets to address this vulnerability on its systems but as of September 2018, only 3 tickets had been closed. JPL systems remained unpatched and exposed to this

[40] The Common Vulnerability Scoring System is a standard measurement system for industries, organizations, and governments used to characterize the severity of vulnerabilities and help prioritize remediation activities. A score of 10 is the highest and deemed critical.

software vulnerability until March 2019 when all the relevant SPL tickets on this vulnerability were closed. During the April 2018 cyberattack, one of the four compromised systems had not been patched for the vulnerability in a timely manner, ultimately resulting in the exfiltration of 23 files containing approximately 500 megabytes of data.

Ineffective IT Security Waiver Process

JPL OCIO provides system administrators the option of requesting waivers when they cannot resolve SPL tickets within 6 months.[41] A waiver allows system administrators to forego correcting a vulnerability or implementing a requirement, such as installing software patches or antivirus software, when they implement alternative security controls to mitigate the risk. Waivers, which do not have expiration dates, must be approved by the IT Security Group Manager, Line Manager, Division Manager (or Director), and the JPL CISO. JPL policy requires system representatives to review waivers annually to ensure any compensating security controls in place associated with the waiver are still applicable.[42] However, we found open waivers were not being reviewed as required by JPL policy.

As of October 2018, JPL's network contained 153 open waivers. Of these, 54 were granted to employees no longer working for JPL and therefore the reason why a waiver was needed or granted likely has been lost. Additionally, of the 13 JPL systems we sampled, 9 contained waivers open between 7 and 11 years. None of the system representatives for these 13 systems could confirm whether the required annual reviews to determine the continued need for the waivers had been conducted, and one system representative was unaware his system had open waivers. Consequently, JPL may be accepting unnecessary risks by failing to assess the validity of open waivers on a regular basis. To the point, in July 2018, JPL OCIO officials said they stopped authorizing new waivers. Table 3 provides a listing and description of the waivers we examined.[43]

[41] JPL OCIO also provides system administrators the option to request a lien when the SPL tickets cannot be resolved within 30 days but will take less than 6 months to resolve. Liens are used for temporary delays in the resolution of vulnerabilities, often due to operational reasons, while waivers are used when mitigating solutions are necessary due to system capability limitations.

[42] JPL Rules 36852 Rev. 15.

[43] We did not attempt to determine whether these long-standing waivers were properly reviewed and granted by JPL OCIO.

Table 3: Long-Standing Waivers for the Sampled Systems

Project[a]	Date Since Waiver First Issued	Description of Waiver
A	January 2007	Waive installation of Patchlink[b]
B	December 2008	Allow system administrators to disable user accounts instead of deleting them, in case personnel with specific skill sets return to the project
C	December 2008	Waive installation of Patchlink[b]
D	December 2008	Allow system administrators to bypass JPL 36852 requirements and to not install patches on a monthly basis as required
E	July 2009	Waive JPL requirement for the monthly application of security-related software updates
F	August 2009	Allow system administrators to omit deleting user accounts
G	March 2010	Waive JPL requirement to change passwords every 90 days
H	September 2011	Waive monthly installation of patches
I	September 2011	Waive installation of antivirus software

Source: NASA OIG analysis of JPL data.

[a] Names of the projects were removed to allow public release of the report.
[b] Patchlink—a patch management software—is no longer in use.

For example, one of the projects has a waiver of JPL IT security requirements to change passwords every 90 days. Instead, the project relies on a designated application and team accounts to share password files, group files, host tables, and other files over the network. The design intent of the application was to provide centralized account information by sharing user and group information across systems. However, security weaknesses in this particular application made the environment susceptible to attacks, such as allowing any user with an account access to any system using the application. In addition, this application does not support password aging.[44] This kind of authentication weakness could allow an attacker to access the user identification of a known authorized user, and the system would give the attacker all the privileges of the authorized user without requiring further authentication. Further, the application is no longer supported by the vendor and software updates are no longer available.[45]

Unnecessary waivers, extended waivers, and outdated compensating security controls expose the JPL network to exploitation by cyberattacks. While we understand the need to issue security waivers for particular systems, allowing waivers to remain open for an indefinite basis without periodic revalidation leaves systems with unresolved vulnerabilities and unapplied patches susceptible to attack. During our review, JPL OCIO confirmed that it is reviewing the appropriateness of all open waivers and plans to complete its review by the end of 2019.

[44] Password aging is a process that ensures passwords are changed after a set amount of time has elapsed.

[45] According to JPL officials, as of April 2019, they were in the process of systematically decommissioning the use of the application on the JPL network.

JPL Log Management Infrastructure Not Operating as Intended

System Administrators Misinterpret Log Analysis Requirements

System administrators play an integral role in the overall security of IT systems within their control. Logs, which record events occurring on a particular system or network, provide valuable information for detecting and investigating malicious activity. Consequently, routine log analysis is a critical practice for identifying security incidents or policy violations and JPL policy requires system administrators to review system log files for suspicious or unusual activity on a regular basis.[46] Since manual review requires a significant amount of time and resources, system administrators are encouraged to use automated tools to review system logs, including the JPL SOC's centralized logging software Splunk ES.[47]

While JPL system administrators responsible for IT security were aware of the requirement to review log files, we found that many of them misunderstood their responsibilities regarding log management and review. Specifically, 9 out of 11 system administrators in our judgmental sample said they believed their routine analysis was no longer necessary once their system logs are sent to Splunk ES for collection and reporting. Moreover, 8 out of 11 system administrators noted they could not review their logs because they did not have access to Splunk ES. However, JPL SOC staff consider system administrators as the "first line of defense" in reviewing log files at the individual system level, with the SOC a secondary resource that reviews aggregated logs created by its intrusion detection systems, analyzes significant events, and responds to alerts generated by its security management tools.[48] These conflicting assertions demonstrate a lack of clear communication regarding the shared responsibilities between system administrators and SOC staff for log management at JPL.

According to NIST, efficient analysis of relevant information depends on a strong understanding of an organization's normal computing baseline, such as typical patterns of usage on systems and networks, and the relative value of such data.[49] Given the size of the JPL institutional and mission networks, analysis of security logs can be a daunting task and requires the ability to interpret the information efficiently and minimize the amount of false positives generated by event monitoring tools. Because system administrators have the most knowledge of their systems and applications, they are best positioned to identify events of significance and forward any concerns to the JPL SOC.

System and application logs not reviewed by system administrators because of a misunderstanding of responsibilities place Agency data at risk of compromise if suspicious activity is not identified in a timely manner. Improved clarity in roles and responsibilities along with improved access to automated tools can help ensure that JPL meets security requirements and reduces the time an attacker may reside within the network undetected.

---

[46] JPL Rules 36852 Rev. 15.

[47] Splunk ES is an analytics-driven security software that aggregates and reviews network and system data to quickly detect and respond to internal and external attacks.

[48] JPL SOC management noted a challenge in obtaining visibility into legacy mission IT systems because these systems cannot be disrupted due to their criticality.

[49] NIST SP 800-92, *Guide to Computer Security Log Management* (September 2006).

Moreover, while JPL has established policies for managing the generation, storage, and analysis of log data, the JPL SOC does not have an effective process to ensure that all system administrators on JPL networks provide the required data for analysis. NIST recommends organizations conduct periodic reviews of processes and procedures to ensure effective log management for detecting threats in their IT environment.[50] Routine log management audits can identify noncompliance with cybersecurity requirements and help develop corrective action plans in a timely manner. Several members of the JPL SOC, however, acknowledged they had no method to determine whether Splunk ES captures all of the required log data. Although JPL has a certification and accreditation process that includes an assessment of system compliance with established log management requirements, these reviews take place only annually. In our opinion, more frequent assessments are necessary until JPL addresses these issues. Without timely identification of compliance with log management requirements for its entire network, JPL's ability to detect bad actors who may have gained access through a mission system is greatly diminished.

Threat-Hunting Capability Needs Improvement

While intrusion detection and prevention systems employed by JPL are necessary to defend against routine intrusions and misuse of computer assets, advanced threats demand a more proactive, efficient approach to incident detection and response. Organizations have responded by implementing threat-hunting programs to aggressively pursue abnormal activity on systems and endpoints for signs of compromise.[51] Threat hunting, which focuses on adversaries already within an organization's networks and systems, provides a framework for analysts seeking to detect such adversaries. However, JPL does not have a formal process for performing such threat-hunting activities, and instead relies on an ad hoc process for searching for intruders.[52]

The effectiveness of an organization's hunting capability can be measured against a "maturity model" that focuses on data quality, security tools analyzing the data, and analysts' skills for conducting a hunt (see Figure 3).[53] We assessed JPL's capabilities based on the cybersecurity tools, processes, and personnel currently in place and determined that JPL falls between the Hunting Maturity Model (HMM) 1 and 2 levels.

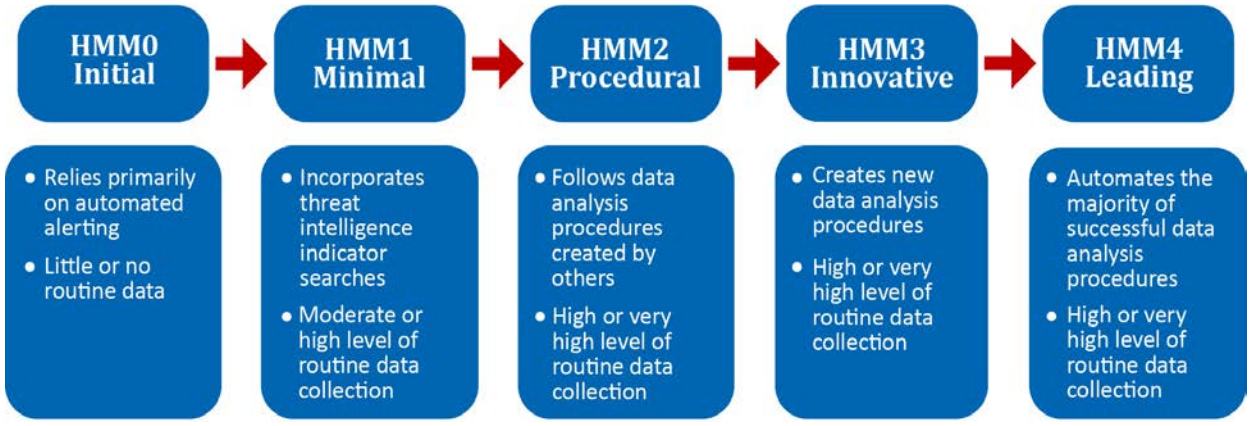
[50] NIST SP 800-92.

[51] While a specific definition of threat hunting has not been established, the term generally refers to the focused effort by organizations to proactively search their networks for advanced threats that possess the intent, capability, and opportunity to evade existing security tools.

[52] The lack of any formal, published methodology is not uncommon. A recent survey by the SANS Institute—a private, for-profit company specializing in information security and a prominent provider of cybersecurity training to professionals, governments, and commercial institutions worldwide—found that 53 percent of respondents had a largely informal hunting process. SANS Institute, *Threat Hunting: Open Season on the Adversary* (April 2016).

[53] David Bianco, "A Simple Hunting Maturity Model," *Enterprise Detection & Response* (blog), October 15, 2015, http://detect-respond.blogspot.com/2015/10/a-simple-hunting-maturity-model.html (accessed on November 15, 2018).

Figure 3: Hunting Maturity Model Levels



Source: NASA OIG presentation of the HMM.

The SANS Institute and other security experts recommend establishing standardized procedures for any successful threat-hunting program. While JPL conducts threat hunting using a variety of cybersecurity tools (e.g., Splunk ES and Snort) to analyze and evaluate threats, along with information sharing feeds (TAXII/STIX), these efforts fall short of a published methodology for SOC analysts.[54] JPL's incident response plan also does not include any specific threat-hunting procedures. A documented process that defines the techniques analysts should follow, including generating hypotheses regarding malicious activity in an IT environment and updating automated detection capabilities based on discovered threats, reduces inefficiencies of random techniques and guides analysts in a more strategic and structured hunt.

JPL SOC analysts we interviewed also described a general process whereby they analyze indicators of compromise and alerts to determine whether an adversary has penetrated a system. While understandable, the SANS Institute cautions threat hunters to avoid becoming overly reliant on indicators of compromise to drive their activities. For example, many threat data feeds lack appropriate context to make them true indicators of compromised systems and following every piece of data could lead an analyst to an incorrect or uncompromised network or system. Instead, the SANS Institute and other industry specialists encourage organizations to develop a formal methodology with clearly defined steps and procedures to improve prioritization of incident investigations, leading to an enhanced security posture.

Inadequate System Administrator Training

JPL has not provided adequate security training to its system administrators. According to GAO, a key component of the government's ability to mitigate and respond to cyber threats is having a qualified, well-trained cybersecurity workforce.[55] According to training data we reviewed, all system

[54] Snort is an open-source network intrusion detection system software for Linux and Windows to detect emerging threats. TAXII and STIX are community-driven technical specifications designed to enable automated information sharing for cybersecurity situational awareness, real-time network defense, and sophisticated threat analysis.

[55] GAO, *Cybersecurity Workforce: Agencies Need to Improve Baseline Assessments and Procedures for Coding Positions* (GAO-18-466, June 14, 2018).

administrators completed the annual mandatory cybersecurity training provided by JPL; however, this basic security awareness training alone does not meet NIST guidelines. Instead, NIST requires that organizations provide security-related technical training specifically tailored for their assigned duties.[56] NIST also requires that organizations:

- provide role-based security training to personnel with assigned security roles and responsibilities before authorizing access to the information system or performing assigned duties,
- provide role-based security training to personnel with assigned security roles and responsibilities when required by information system changes,
- define the frequency to provide refresher role-based security training thereafter to personnel with assigned security roles and responsibilities, and
- provide refresher role-based security training to personnel with assigned security roles and responsibilities with the organization-defined frequency.

As of April 2019, JPL did not have a role-based training program, provide additional IT security training for system administrators, nor fund their IT security certifications.[57] JPL OCIO officials said they plan to implement the role-based training program by July 2019; however, this program faces several challenges, including freeing up personnel to attend the training and the need for additional funding associated with the planned role-based training courses.[58]

JPL Has Not Fully Implemented Effective Incident Response Procedures

Improved Staffing Coverage Needed to Handle Alerts and Respond to Incidents

As previously discussed, the JPL SOC provides day-to-day monitoring of networks and information systems, including real-time analysis of logs generated by its intrusion detection systems. To accomplish this task, the SOC utilizes a series of network sensors to detect events and incidents, as well as security event and information management software to correlate sensor data and IT security logs. Although these tools remain an integral component of an incident response program, their effectiveness also depends on the timely analysis and interpretation of data produced. JPL currently staffs its SOC during regular business hours and maintains one analyst on call to respond to after-hours alerts. Conversely, the NASA SOC provides a dedicated IT security staff 24 hours per day, 7 days a week for monitoring agency networks in conjunction with its suite of intrusion detection tools and sensors. Data from the NASA SOC incident management system, however, indicates that JPL handles a comparable number of incidents with other Agency Centers. Table 4 details the number of incidents reported in 2017 for each Center using common incident categories previously adopted by DHS's United States Computer Emergency Readiness Team (US-CERT) for federal reporting guidelines.

[56] NIST SP 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013).

[57] JPL completed a pilot role-based training program in December 2017.

[58] The training program implementation was delayed from February 2019 to July 2019 due to the 35-day government shutdown from December 2018 through January 2019.

Table 4: NASA Incidents by US-CERT Category for 2017

US-CERT Category	AFRC	ARC	GRC	GSFC	HQ	JPL	JSC	KSC	LRC	MSFC	SSC
CAT 1—Unauthorized Access[a]	27	53	22	133	102	133	131	50	54	84	19
CAT 2—Denial of Service[b]	0	1	1	17	1	1	3	0	2	3	0
CAT 3—Malicious Code[c]	13	20	19	72	21	8	64	63	15	35	10
CAT 4—Improper Usage[d]	2	6	7	21	5	6	80	10	37	25	6
Total	**42**	**80**	**49**	**243**	**129**	**148**	**278**	**123**	**108**	**147**	**35**

Source: NASA SOC incident management system.

Note: Armstrong Flight Research Center (AFRC), Ames Research Center (ARC), Glenn Research Center (GRC), Goddard Space Flight Center (GSFC), Headquarters (HQ), Jet Propulsion Laboratory (JPL), Johnson Space Center (JSC), Kennedy Space Center (KSC), Langley Research Center (LRC), Marshall Space Flight Center (MSFC), and Stennis Space Center (SSC).

[a] CAT 1—Unauthorized Access is when an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource.
[b] CAT 2—Denial of Service is an attack that successfully prevents or impairs the normal authorized functionality of networks, systems, or applications by exhausting resources. This activity includes being the victim or participating in the Denial of Service.
[c] CAT 3—Malicious Code is the successful installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application.
[d] CAT 4—Improper Usage is when a person violates acceptable computing use policies.

The severity of an incident often depends on the length of time an intruder is able to maintain a foothold within an organization's network, so round-the-clock availability of incident responders is critical to timely containment of suspicious activity and improvement of JPL's incident response capability.

Although the JPL SOC tries to leverage help from other teams within the JPL OCIO and NASA SOC when necessary, they do not outsource any incident response and detection activities. While incident response teams can structure themselves using a variety of models, adopting a more flexible staffing approach could reduce the burden on permanent staff during times of increased activity and investigation. For example, according to a 2014 SANS Institute incident response survey, 50 percent of respondents retain additional support staff to handle incidents deemed critical.[59] Given the high number of incidents and limited staff, leveraging talent and expertise from non-JPL SOC resources could fill possible detection capability gaps.

[59] SANS Institute, *Incident Response: How to Fight Back* (August 2014).

JPL's Incident Response Plan Does Not Include Recommended Elements

It is widely acknowledged that intrusions are inevitable and that organizations need to take appropriate steps to detect and respond to such incidents once they occur. The development of an incident response policy that identifies roles and responsibilities, defines which events should be considered incidents, and establishes reporting requirements is an integral component of an effective response capability. According to NIST, an incident response policy serves as the "foundation" of an organization's incident response program and organizations should develop a corresponding plan to provide a roadmap for policy implementation.[60] While JPL generally addressed most of the recommended elements in its incident response plan, the plan needs additional updates to ensure effective implementation of its incident response capabilities. Specifically, the plan does not include, or only partially includes, the following elements:

- statement of management commitment
- performance measures
- mission statement (partially included)
- metrics for measuring the incident response capability and its effectiveness
- roadmap for maturing the incident response capability
- how the program fits into the overall organization
- annual review

In a rapidly evolving IT environment, JPL's inclusion of these additional elements will help ensure it maintains a complete incident response plan aligned with its incident response goals. For example, a roadmap discussing the adaptability of JPL's incident management program, including identification of improvements and upgrades to detection software, staffing adjustments to address increased alert activity, and timelines for updating the incident response plan will help ensure that the OCIO continually improves as new threats emerge. Similarly, inclusion of performance measures—such as the average length of time between an incident being reported and the incident being closed for each attack or how long it took to report the incident to appropriate external entities (e.g., NASA SOC)—will help JPL identify problems and deficiencies in its resource allocation and assess the overall effectiveness of its incident response program.

An updated incident response plan will also help streamline JPL's process for identifying and managing cyberattacks and provide clear procedures for current and future staff. Our discussions with JPL SOC analysts and investigators revealed that most rely on their personal experience to respond to alerts, identify false positives, and assess abnormal network behavior. They described a process of informal discussions and subjective analysis methods for carrying out their detection responsibilities. While we recognize the benefit of identifying credible alerts and responding to incidents on the basis of institutional experience, we believe it places undue reliance on individual analysis and impedes the long-term strategy of maintaining a mature incident response capability that provides clear direction for SOC analysts.

[60] NIST SP 800-61 Rev. 2, *Computer Security Incident Handling Guide* (August 2012).

Delayed Response to an Advanced Persistent Threat Attack

After detection and initial analysis of an incident, the next step in the incident response process should be containment of the attack to limit the extent of any damage. Containment strategies may include identifying all attack paths, performing a system shutdown, and disconnecting a system from the network. Subsequently, the threat must be eradicated from the environment, an assessment and analysis of exploited vulnerabilities undertaken, malware and affected files removed, and security patches applied. Most of these steps require sophisticated forensic expertise and tools that when not available in-house should be in place through service agreements with specialized providers.

In response to the April 2018 incident, an advanced persistent threat attack, NASA SOC requested an independent assessment from DHS US-CERT to determine the scope of the attack and remove the adversary from JPL's network. Although JPL had closed off the known path of attack and disabled the account targeted by the adversary, NASA sought additional assurance regarding the success of JPL's containment and eradication efforts and the security of the network. However, according to NASA SOC personnel, JPL was concerned with inadvertent access to its corporate network and feared disruption of mission operations. In addition, JPL was unfamiliar with DHS's standard engagement procedures. Collectively, resolution of these issues resulted in DHS being unable to perform scans of the entire network until 4 months after the incident was detected. Once DHS performed the scans, it determined there were no other attack paths and deemed the network clean; however, the delay in executing the eradication steps left NASA data and systems vulnerable to potential additional harm.

JPL Process for Sharing Lessons Learned Needs Improvement

NASA policy has long encouraged sharing of knowledge "to continuously improve the performance of NASA in implementing its mission."[61] For example, NASA's Safety Culture Handbook describes a learning culture as one where employees collect, assess, and share information in an atmosphere of open communication and shared values and lessons.[62] NASA's IT Security Handbook for incident management also encourages a program that addresses sharing of cyber threat information within the Agency.[63] Documenting and sharing information to help prevent future incidents is a critical component of an effective incident response program. However, we found JPL's current initiatives fall short of the learning culture NASA strives to implement across the Agency.

Although JPL develops post-incident bulletins, applies lessons learned directly into operations on an ad-hoc basis, or holds meetings following particular incidents, the specific lessons may not be reaching their intended audience. We spoke with 17 system administrators who provided inconsistent responses regarding the existence and availability of such lessons learned information.[64] While some stated that no information was shared, others indicated that the JPL OCIO shares information infrequently and,

[61] NASA Policy Directive 7120.6, *Knowledge Policy on Programs and Projects* (November 26, 2013).

[62] NASA Technical Handbook 8709.24, *NASA Safety Culture Handbook* (November 23, 2015).

[63] NASA IT Security Handbook 2810.09-02A, *NASA Information Security Incident Management Handbook* (March 17, 2017).

[64] In addition to the 11 system administrators in our judgmental sample, we conducted a survey to which we received responses from 6 additional system administrators.

until recently, failed to hold regular meetings following an incident. According to NIST, learning and improving are key components of an organization's incident response process and it considers lessons-learned meetings "extremely helpful" in improving security and the incident handling process.[65] These meetings provide valuable training for team members and identify indicators for potential future incidents. The SANS Institute also encourages the development of a report or Power Point presentation that summarizes information relating to the scope of security incidents, work performed to recover from the incident, and identification of areas that were effective or need improvement.[66] Accordingly, we believe that the JPL SOC needs to develop more effective mechanisms for sharing lessons learned to ensure that stakeholders responsible for protecting IT assets are receiving the appropriate information in a timely manner.

[65] NIST SP 800-61 Rev. 2.

[66] SANS Institute, *The Incident Handler's Handbook* (December 5, 2011).

NASA Lacks Adequate Oversight of JPL Network Security

NASA's contract with Caltech does not provide the Agency with proper oversight of JPL's IT environment to ensure the protection and management of NASA data, applications, and systems. As the contractor who operates JPL on NASA's behalf, Caltech maintains control over the selection and implementation of security controls for data, systems, and applications maintained on the JPL network. Despite not having direct control over these assets, NASA's interest in the security of information systems that collect, process, and transmit Agency data demands proper oversight of JPL's IT environment to ensure that security controls applied to systems and applications are appropriate.[67]

NASA Unable to Monitor Assets on the JPL Network

Although the contract between NASA and Caltech requires JPL to report certain types of IT security incidents to the Agency through the NASA SOC incident management system, no controls are in place to ensure that JPL complies with this requirement. Moreover, NASA does not have access to JPL's incident management system nor has ever undertaken an audit of the system.

In an effort to ensure proper oversight of incidents occurring on JPL's network, the NASA SOC drafted a Service Level Objectives agreement with the JPL SOC that defines reporting responsibilities and expectations. However, the agreement has not been finalized, and we believe additional clarity regarding the scope of reportable incident types is needed to ensure the Agency ultimately receives the agreed-upon information. We requested a list of incidents JPL categorized as "non-reportable" for a 6-month period in 2018 and were unable to determine whether these incidents, which included reportable event types listed in the agreement, should have been shared with the NASA SOC. Moreover, while the NASA SOC informed us that all malware incidents should be reported by JPL, 17 out of 91 incidents included in the "non-reportable" list JPL provided were categorized as "malicious code," suggesting inconsistent interpretations of generally defined terms in the agreement. Without improved clarity as to what constitutes a reportable incident, NASA may not be receiving all of the data needed to ensure adequate protection of sensitive Agency information.

NASA Security Operations Center at Ames Research Center

Source: NASA.

[67] In 2009, GAO similarly identified the lack of contractual provisions providing NASA with effective oversight of Caltech's IT program and implementation of security controls and recommended the Agency include all security requirements in the JPL contract. GAO, *Information Security: NASA Needs to Remedy Vulnerabilities in Key Networks* (GAO-10-4, October 15, 2009).

NASA IT security officials also expressed concern to us about the Agency's inability to directly monitor NASA assets on the JPL network. Specifically, the NASA SOC would like to enhance data sharing with JPL and develop the ability to directly monitor NASA assets on the JPL network. Caltech, however, has previously resisted such efforts, asserting privacy concerns when the Agency sought to increase its visibility into JPL networks. Furthermore, while NASA SOC performs vulnerability scanning of the JPL network and notifies JPL of any suspicious activity, NASA SOC does not check whether the vulnerabilities have been remediated. This lack of insight into JPL's follow-up efforts prevents the Agency from providing proper oversight of JPL's security controls.

Despite these long-standing concerns, NASA did not explicitly include these data sharing or oversight requirements in the 5-year contract it signed with Caltech in October 2018. Moreover, IT security was one of the issues left unresolved when the new contract was implemented, with the Agency and Caltech agreeing to continue negotiating these issues through approval of an IT Transition Plan called for in the contract. This plan, along with an OCIO implementation plan, describe Caltech's proposed approach to fulfilling its new requirements and meeting the intent of NASA's IT security policies.[68] Although implementation plans for the new contract have been established between JPL and other NASA offices such as the Office of Safety and Mission Assurance and the Office of the Chief Engineer to address safety and mission-related issues, as of March 2019 the Agency and Caltech continued to disagree on how to approach the new IT security policies and requirements. Major outstanding issues included implementing Continuous Diagnostics and Mitigation at JPL, transitioning JPL systems off the government domain and onto a private domain, and establishing compliance of JPL websites with relevant regulatory requirements, including the Federal Information Security Modernization Act of 2014.[69]

Apart from these ongoing negotiations, NASA IT security officials said they are working to improve their oversight and control of JPL network security. Some of the desired improvements include incident response practices consistent with NASA SOC practices; 24 hours a day, 7 days a week event monitoring; participation in forensics aspects of incident remediation; and improved information sharing, including JPL's participation in NASA's collection of system security plans from across the Agency into one centralized location for improved coordination and visibility into JPL system security.

[68] Security requirements include NASA Policy Directive 2800.1B, *Managing Information Technology* (March 21, 2008); NASA Procedural Requirements 2810.1A, *Security of Information Technology (Revalidated with Change 1, dated May 19, 2011)* (May 16, 2006); and the Federal Information Security Modernization Act of 2014, and were not specifically listed in the previous contract.

[69] Continuous Diagnostics and Mitigation is a federal IT security program developed by OMB and administered by DHS that provides agencies with IT security tools to identify security issues and help meet federal security requirements. NASA started implementing Continuous Diagnostics and Mitigation tools in November 2016 and expects the software to, among other things, help identify assets connected to its networks, support patch and vulnerability management, and increase visibility over all networks.

CONCLUSION

As the center of NASA's interplanetary robotic research efforts, JPL and its IT systems maintain a wide public internet presence while supporting missions and networks that control spacecraft, collect and process scientific data, and perform critical operational functions. In spite of its efforts to protect these assets, critical vulnerabilities remain that place JPL at risk of cyber intrusions resulting in the theft of critical information. We identified a series of weaknesses in JPL's system of security controls that collectively diminish its ability to effectively prevent, detect, and mitigate cyberattacks targeting its IT systems and networks. Several of these weaknesses were exploited during an April 2018 security breach that resulted in the loss of approximately 500 megabytes of data. The inability to protect against cyberattacks in general and advanced persistent threats in particular places the Agency's status as a global leader in space exploration and aeronautics research at risk. Accordingly, effective network security requires a system of sound IT security controls.

In addition, NASA does not have sufficient oversight into JPL's system of security controls to effectively monitor and protect the Agency's assets. NASA is responsible for ensuring its IT assets are protected from unauthorized or inappropriate access, including assets on the JPL network managed by Caltech pursuant to NASA's contract with the university. Improvements to JPL's security controls and increased oversight by NASA is crucial to ensuring the confidentiality, integrity, and availability of Agency data.

RECOMMENDATIONS, MANAGEMENT'S RESPONSE, AND OUR EVALUATION

To improve JPL network security controls and provide NASA greater oversight, we recommended the Director of the NASA Management Office instruct the JPL Chief Information Officer to:

1. Require all system administrators to review and update the ITSDB to ensure all system components are properly registered in the database, and require the JPL CITO to periodically review the ITSDB for compliance with this requirement.

2. Segregate shared environments connected to the network gateway for all partners accessing the JPL network and monitor partner activity when accessing the network.

3. Review and update ISAs for all partners connected to the network gateway to ensure they are up-to-date and made available to the NASA OCIO.

4. Require the JPL CITO to identify and remediate weaknesses in the SPL ticket process and provide periodic aging reports to the JPL CIO detailing the status of open SPL tickets, pending patches, and outdated security waivers.

5. Require the JPL CITO to complete its validation and updates of open waivers, perform annual reviews to ensure system representatives are validating the need for the waiver, and provide NASA documentation of these waivers.

6. Clarify the division of responsibility between the JPL OCIO and system administrators for conducting routine log reviews and monitor their compliance with this requirement on a more frequent basis.

7. Implement the planned role-based training program by July 2019.

8. Establish a formal, documented threat-hunting process that includes roles and responsibilities, standard processes for conducting a hunt, and metrics to track success.

9. Develop and implement a comprehensive strategy for institutional IT knowledge and incident management that includes the dissemination of lessons learned to system administrators and other appropriate personnel.

We also recommended the NASA Chief Information Officer:

10. Include requirements in the pending IT Transition Plan for implementation of continuous monitoring tools that provide the NASA SOC with oversight of JPL network security practices to ensure they adequately protect NASA data, systems, and applications.

We provided a draft of this report to NASA management who concurred with 9 of our 10 recommendations. We consider management's comments to those 9 recommendations responsive; therefore, the recommendations are resolved and will be closed upon completion and verification of the proposed corrective actions.

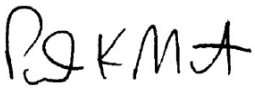
Management did not concur with Recommendation 8, stating that it is not the responsibility of Caltech as a NASA contractor to implement a threat-hunting process. Instead, NASA management stated that it will move forward to establish this capability after the National Institute of Standards and Technology provides federal agencies with formal threat-hunting guidance.

Given that management indicated it intends to implement the recommendation upon receiving additional guidance, we believe it could be resolved if the Agency provides an anticipated date for implementing the threat-hunting capability. Until then, this recommendation will remain unresolved pending discussion with the Agency.

Management's comments are reproduced in Appendix C. Technical comments provided by management and revisions to address security concerns regarding public release of this report have also been incorporated as appropriate.

Major contributors to this report include Raymond Tolomeo, Science and Aeronautics Research Director; Gerardo Saucedo, Project Manager; Joseph Bennett; Anh Doan; Cyrus Geranmayeh; Jiang Yun Lu; Behshad Sedighi; and Lauren Suls.

If you have questions 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 performed this audit from April 2018 through April 2019 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.

During our audit, we interviewed JPL IT representatives and reviewed JPL's IT network mapping to obtain an understanding of the structure of JPL's networks and its security organizational and operational processes. We compared the system inventory listing and verified it with various source databases, such as the ITSDB and ASR. We also obtained lists of critical vulnerabilities from sources such as Caltech audit reports, JPL SOC incident reports, and the Cyber Hygiene Assessment of NASA conducted by DHS's National Cybersecurity Assessments and Technical Services. The DHS Cyber Hygiene report includes JPL external facing networks between November 2017 and April 2018 and highlighted the most problematic external facing networks. From these reports, we selected and reviewed a sample of 13 systems and their System Security Plans, as well as the related SPL tickets. Our selection included external facing systems, mission systems, and other systems from the JPL corporate network. We traced these systems to their appropriate system security plans, which encompassed 3,541 systems in total. In addition, we interviewed the system administrators and system representatives of the selected 13 systems, as well as process owners of the training module, patch management, vulnerability scanning, SPL tickets, waivers and liens, foreign national access, and incident response.

We reviewed Service Level Objectives established between JPL SOC and NASA SOC regarding the scope and expectations for delivery of event and incident documentation and reporting. We also interviewed JPL SOC personnel regarding JPL's documented incident response processes. In addition, we interviewed NASA OCIO and NASA SOC officials to understand the Agency's oversight roles and responsibilities towards incident reporting and response. Finally, we reviewed federal, NASA, and JPL criteria, policies, and procedures and supporting documentation, prior audit reports, external reviews, and other documents related to cybersecurity. The documents we reviewed included, but were not limited to, the following:

- OMB Circular A-130, *Management of Federal Information Resources* (February 8, 1996)
- DHS Binding Operational Directive 15-01, *Critical Vulnerability Mitigation Requirement for Federal Civilian Executive Branch Departments and Agencies' Internet-Accessible Systems* (May 21, 2015)
- NIST, *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1* (April 16, 2018)
- NIST Special Publication (SP) 800-37 Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach* (February 2010)
- NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View* (March 2011)
- NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems* (August 2002)

- NIST SP 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013)
- NIST SP 800-53A Rev. 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans* (December 2014)
- NIST SP 800-61 Rev. 2, *Computer Security Incident Handling Guide* (August 2012)
- NASA Policy Directive (NPD) 1000.3E, *The NASA Organization w/Change 39 (approved October 26, 2018)* (April 15, 2015)
- NPD 2800.1B, *Managing Information Technology* (March 21, 2008)
- NPD 2810.1E, *NASA Information Security Policy* (July 14, 2015)
- NPD 7120.6, *Knowledge Policy on Programs and Projects* (November 26, 2013)
- NASA Technical Handbook 8709.24, *NASA Safety Culture Handbook* (November 23, 2015)
- NASA Procedural Requirements 2800.1B, *Managing Information Technology* (March 20, 2009)
- NASA Procedural Requirements 2810.1A, *Security of Information Technology (Revalidated with Change 1, dated May 19, 2011)* (May 16, 2006)
- NASA IT Security Handbook 2810.09-02A, *NASA Information Security Incident Management* (March 17, 2017)
- JPL Rules 35506 Rev. 8, *Anomaly Resolution* (May 26, 2016)
- JPL Rules 36852 Rev. 15, *JPL Cybersecurity Requirements* (August 21, 2017)
- JPL Rules 62013 Rev. 20, *JPL Information Technology Contingency Plan (ITCP)* (April 19, 2018)
- JPL Rules 78754 Rev. 0, *JPL Cybersecurity Strategy* (December 15, 2014)

Use of Computer-Processed Data

We used computer-processed data to perform this audit, and that data was used to materially support findings, conclusions, and recommendations. In order to assess the quality and reliability of the data, we compared the information with other available supporting documents, corroborating it with program documents and input from various program officials. From these efforts, we believe the information we obtained is sufficiently reliable for this report.

Review of Internal Controls

We reviewed and evaluated internal controls related to JPL IT network security processes, as well as those related to our sample of 13 information systems. We examined controls related to cybersecurity including the identification, protection, detection, and response of IT assets. The control weaknesses we identified are discussed in this report. Our recommendations, if implemented, will correct the identified control weaknesses.

Prior Coverage

During the last 7 years, NASA OIG and GAO have issued 24 reports of significant relevance to the subject of this report. Unrestricted reports can be accessed at https://oig.nasa.gov/audits/auditReports.html and https://www.gao.gov, respectively.

NASA Office of Inspector General

NASA's Process for Acquiring Information Technology Security Assessment and Monitoring Tools (IG-13-006, March 18, 2013)

Federal Information Security Management Act: Fiscal Year 2013 Evaluation (IG-14-004, November 20, 2013)

NASA's Management of its Smartphones, Tablets, and Other Mobile Devices (IG-14-015, February 27, 2014)

Security of NASA's Publicly Accessible Web Applications (IG-14-023, July 10, 2014)

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

Federal Information Security Management Act: Fiscal Year 2014 Evaluation (IG-15-004, November 13, 2014)

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

Federal Information Security Management Act: Fiscal Year 2015 Evaluation (IG-16-002, October 19, 2015)

NASA's Management of the Near Earth Network (IG-16-014, March 17, 2016)

Review of NASA's Information Security Program (IG-16-016, April 14, 2016)

Report Mandated by the Cybersecurity Act of 2015 (IG-16-026, July 27, 2016)

Federal Information Security Modernization Act: Fiscal Year 2016 Evaluation (IG-17-002, November 7, 2016)

Industrial Control System Security within NASA's Critical and Supporting Infrastructure (IG-17-011, February 8, 2017)

Federal Information Security Modernization Act: Fiscal Year 2017 Evaluation (IG-18-003, November 6, 2017)

Audit of NASA's Security Operations Center (IG-18-020, May 23, 2018)

Government Accountability Office

Federal Information Security: Mixed Progress in Implementing Program Components; Improved Metrics Needed to Measure Effectiveness (GAO-13-776, September 26, 2013)

Information Security: Agencies Need to Improve Cyber Incident Response Practices (GAO-14-354, April 30, 2014)

Export Controls: NASA Management Action and Improved Oversight Needed to Reduce the Risk of Unauthorized Access to Its Technologies (GAO-14-690T, June 20, 2014)

Federal Information Security: Agencies Need to Correct Weaknesses and Fully Implement Security Programs (GAO-15-714, September 29, 2015)

Information Security: Agencies Need to Improve Controls over Selected High-Impact Systems (GAO-16-501, May 18, 2016)

Federal Chief Information Security Officers: Opportunities Exist to Improve Roles and Address Challenges to Authority (GAO-16-686, August 26, 2016)

Federal Information Security: Weaknesses Continue to Indicate Need for Effective Implementation of Policies and Practices (GAO-17-549, September 28, 2017)

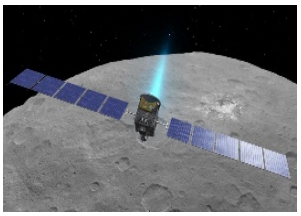
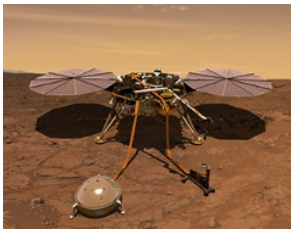
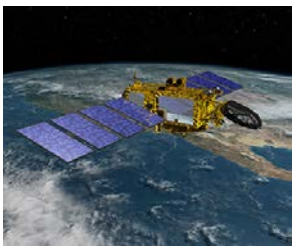
NASA Information Technology: Urgent Action Needed to Address Significant Management and Cybersecurity Weaknesses (GAO-18-337, May 22, 2018)

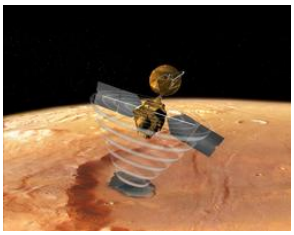
Cybersecurity Workforce: Agencies Need to Improve Baseline Assessments and Procedures for Coding Positions (GAO-18-466, June 14, 2018)

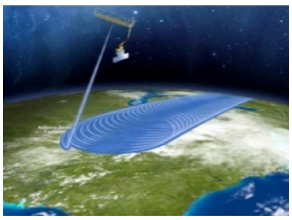
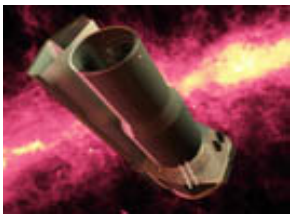
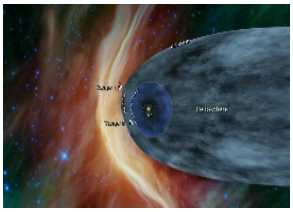
APPENDIX B: MISSIONS SUPPORTED BY JPL'S NETWORK

JPL's network supports a variety of NASA missions currently in operation. Table 5 lists the mission support areas and provides a description and the status of those missions.

Table 5: Missions Supported by the JPL Network

Mission	Description	Status
DAWN 	Part of NASA's Discovery Program, Dawn was a space probe mission to the two most massive bodies in the main asteroid belt—Vesta and Ceres. Dawn orbited and explored the protoplanet Vesta in 2011 and 2012, and it has been in orbit around the dwarf planet Ceres since March 2015.	Launched in 2007, Dawn ended its mission on November 1, 2018. Currently it is in orbit around Ceres, where it will remain for decades.
DSN NOCC 	DSN NOCC (Network Operations Control Center) is responsible for scheduling the DSN's resources and monitoring all multi-mission spacecraft tracking activities in real-time. Operations performs this job with computer systems at JPL connected to over 100 computers at Goldstone, California, and in Australia and Spain.	Continues to provide operations support to DSN.
InSight 	NASA's InSight (Interior exploration using Seismic Investigations, Geodesy, and Heat Transport) is a Mars lander designed to study in-depth the "inner space" of Mars—its crust, mantle, and core.	Launched May 5, 2018, InSight landed on Mars on November 26, 2018, and is in the process of fully deploying its scientific instruments for data collection.
JASON 	Extending the timeline of ocean surface topography measurements begun by TOPEX/Poseidon, Jason-1, and the Ocean Surface Topography Mission on the Jason-2 satellite, Jason-3 is the fourth in a series of U.S.-European satellite missions. Jason-3 will make highly detailed measurements of sea-level on Earth to gain insight into ocean circulation and climate change.	Launched in 2016, Jason-3 remains in operation.

Mission	Description	Status
Juno 	Juno's primary goal is to reveal information about Jupiter's formation and evolution. Using long-proven technologies on a spinning spacecraft placed in an elliptical polar orbit, Juno will observe Jupiter's gravity and magnetic fields, atmospheric dynamics and composition, and evolution.	Launched in 2011, the Juno spacecraft successfully entered Jupiter's orbit in 2016 with its science operations extended to 2021.
Mars Odyssey 	The Mars Odyssey spacecraft is part of NASA's Mars Exploration Program, a long-term effort of robotic exploration of the Red Planet. The Odyssey has spent more time than any other spacecraft in history in orbit around Mars collecting data on its climate and geology and served as a key communications relay for the Mars Exploration Rovers Spirit and Opportunity.	Launched in 2001, Odyssey transmitted 85 percent of the data from the Spirit and Opportunity Mars rovers to Earth and will continue to provide relay support for the Mars Curiosity Rover.
MGSS	MGSS (Multi-Mission Ground Systems and Services) Program Office manages the Advanced Multi-Mission Operations System, which is a set of mission operations and data processing capabilities for robotic missions through an "Ops in a Box" approach utilized by more than 50 missions (including planetary exploration, deep space, earth science, heliophysics, and astrophysics).	Continues to provide operations support and is used by NASA, the European Space Agency, industry, and academia.
MRO 	The MRO (Mars Reconnaissance Orbiter) is a multipurpose spacecraft designed to advance our understanding of Mars through detailed observation, examine potential landing sites for future surface missions, and provide a high-data-rate communications relay for those missions.	Launched in 2005, the orbiter continues to support the Mars Exploration Program by providing communications support to future Mars missions during approach, navigation, and relay.
MSL 	The MSL's (Mars Science Laboratory) Curiosity rover mission will be used to determine whether Mars ever was, or is, habitable to microbial life. The Curiosity rover—a large, mobile laboratory—was placed at the Gale Crater using precision landing technology that made one of Mars' most intriguing regions a viable destination for the first time.	Launched in 2011, Curiosity landed on Mars in 2012 and continues to explore Mars' surface.

Mission	Description	Status
NEOWISE 	Funded by NASA's Planetary Science Division, the NEOWISE project is the asteroid-hunting portion of the Wide-field Infrared Survey Explorer mission.	Launched in December 2009, NEOWISE survey operations are continuing in 2019.
SMAP 	SMAP (Soil Moisture Active Passive) is an orbiting observatory designed to measure the amount of water in the top 2 inches of soil everywhere on Earth's surface over a 3-year period, every 2 to 3 days. This permits changes to be observed over timescales ranging from major storms to repeated measurements of changes over the seasons.	Launched in 2015, mission operators communicate with the observatory and receive instrument data through NASA's Near Earth Network.
Spitzer 	Designed to study the early universe in infrared light, the Spitzer Space Telescope is the first to see light from a planet outside our solar system. Spitzer has also made important discoveries about comets, stars, exoplanets, and distant galaxies.	Launched in 2003 and originally built to last for a minimum of 2.5 years, Spitzer is expected to continue operating until late in this decade.
Voyager 	Voyager 1 and Voyager 2 are twin spacecraft launched by NASA separately in the summer of 1977. Their primary mission was the exploration of Jupiter and Saturn. Both spacecraft continue to send scientific information about their surroundings through the DSN.	Launched in 1977, Voyager 1 is in interstellar space and Voyager 2 is currently in the outermost layer of the heliosphere.

Source: NASA OIG presentation of Agency information.

APPENDIX C: MANAGEMENT'S COMMENTS

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

JUN 13 2019

Reply to Attn of: NASA Management Office

TO: Assistant Inspector General for Audits

FROM: Chief Information Officer
Director, NASA Management Office

SUBJECT: Agency Response to OIG Draft Report, "Cybersecurity Management and Oversight at the Jet Propulsion Laboratory" (A-18-012-00)

NASA appreciates the opportunity to review and comment on the Office of Inspector General (OIG) draft report entitled, "Cybersecurity Management and Oversight at the Jet Propulsion Laboratory" (A-18-012-00) dated May 1, 2019.

In the draft report, the OIG makes a total of ten recommendations intended to improve network security controls at the Jet Propulsion Laboratory (JPL).

The JPL is NASA's only Federally Funded Research and Development Center (FFRDC). While the Lab is sponsored by NASA, it is operated by a contractor, the California Institute of Technology (Caltech), under a contract between NASA and Caltech. The NASA Management Office (NMO) manages this contract and provides on-site Agency oversight of Caltech's operations at the Lab. In formulating the Agency's response to OIG's recommendations, NMO and OCIO consulted with Caltech and considered Caltech's inputs to the Agency's responses below. Specifically, the OIG recommends that:

To improve JPL network security controls and provide NASA greater oversight, the OIG recommends the Director of the NASA Management Office instruct the JPL Chief Information Officer to:

Recommendation 1: Require all system administrators to review and update the Information Technology Security Database (ITSDB) to ensure all system components are properly registered in the database, and require the JPL Cyber/Identity Technologies and Operations Group (CITO) to periodically review the ITSDB for compliance with this requirement.

Management's Response: NASA Concurs. Caltech indicated that the JPL Cyber/Identity Technologies and Operations Group (CITO) will conduct semiannual assessments of the inventory listed in the security plans to ensure that system components are registered properly in the ITSDB. Any deficiencies will be recorded in

Security Problem Log (SPL) tickets, and the JPL OCIO will work with cognizant system administrators to address the plan of action and milestones (POAMs). The NMO, in coordination with the NASA OCIO, will oversee the execution of the recommendation response.

Estimated Completion Date: September 30, 2019

Recommendation 2: Segregate shared environments connected to the network gateway for all partners accessing the JPL network and monitor partner activity when accessing the network.

Management's Response: NASA Concurs. Caltech indicated that JPL moved systems that partners access (e.g., telemetry tracking systems) to the network DMZ and segmented remote access systems to increase JPL's visibility of lateral movement. Additionally, JPL is reviewing all Interconnection Security Agreements (ISA) to determine whether any other systems require segregation. All ISAs will be updated to reflect the recommended changes, and JPL will work via the NMO to obtain NASA concurrence on the ISA updates. The NMO, in coordination with the NASA OCIO, will oversee the execution of the recommendation response.

Estimated Completion Date: January 15, 2020

Recommendation 3: Review and update ISAs for all partners connected to the network gateway to ensure they are up-to-date and made available to the NASA OCIO.

Management's Response: NASA Concurs. Caltech indicated that JPL will review all ISAs and use the guidelines outlined in the NIST SP800-47 "Security Guide for Interconnecting IT Systems." JPL will work with the Government Authorizing Official (AO) and/or the AO Designated Representative (AODR) for each security plan access and obtain AO/AODR concurrence on accepting the risks identified. JPL will develop POAMs and schedules for updating each of the ISAs. Lastly, JPL will work with each project AO for review and signature of each updated ISA. The NMO, in coordination with the NASA OCIO, will oversee the execution of the recommendation response.

Estimated Completion Date: January 15, 2020

Recommendation 4: Require the JPL CITO to identify and remediate weaknesses in the SPL ticket process and provide periodic aging reports to the JPL CIO detailing the status of open SPL tickets, pending patches, and outdated security waivers.

Management's Response: NASA Concurs. Caltech has indicated that the JPL Cyber/Identity Technologies and Operations Group (CITO), as a normal course of business, provides reports to the JPL CIO and creates POAMs to remediate issues or increase capabilities when identified. The CITO will review the SPL ticket process to

identify and remediate weaknesses and will work with the JPL CIO to determine additional reporting requirements. JPL increased its scrutiny over waivers and the waiver process. JPL will provide the AO/AODR with justification and status of existing or any new waiver requests once NASA designates its AOs and AODRs. The NMO, in coordination with the NASA OCIO, will oversee the execution of the recommendation response.

Estimated Completion Date: September 30, 2019

Recommendation 5: Require the JPL CITO to complete its validation and updates of open waivers, perform annual reviews to ensure system representatives are validating the need for the waiver, and provide NASA documentation of these waivers.

Management's Response: NASA Concurs. Caltech has indicated that JPL will ensure the JPL Audit and Vulnerability Assessment Team (AVAT) reviews all waivers during the annual Certification & Accreditation (C&A) process and as part of the triennial independent review, conducted by JPL, on a cyclical basis for all Moderate and High system security plans. Additionally, JPL will conduct an initial out-of-cycle review of all waivers and provide NASA with a current justification and status. The NMO, in coordination with the NASA OCIO, will oversee the execution of the recommendation response.

Estimated Completion Date: September 30, 2019

Recommendation 6: Clarify the division of responsibility between the JPL OCIO and system administrators for conducting routine log reviews and monitor their compliance with this requirement on a more frequent basis.

Management's Response: NASA Concurs. Caltech has indicated that JPL will implement an annual System Administrator (SA) role-based training, beginning July 2019, for all system administrators. During this annual training, JPL will clarify the division of responsibilities between the JPL OCIO and the SAs. The JPL Chief Information Security Officer (CISO) ISO will ensure the JPL Audit and Vulnerability Assessment Team (AVAT) monitors the SA-log review more frequently and in accordance with the JPL cybersecurity requirements. The NMO, in coordination with the NASA OCIO, will oversee the execution of the recommendation response.

Estimated Completion Date: September 30, 2019

Recommendation 7: Implement the planned role-based training program by July 2019.

Management's Response: NASA Concurs. Caltech has indicated that JPL will implement an annual System Administrator (SA) role-based training beginning July

2019 for all system administrators. The NMO, in coordination with the NASA OCIO, will oversee the execution of the recommendation response.

Estimated Completion Date: July 30, 2019

Recommendation 8: Establish a formal, documented threat-hunting process that includes roles and responsibilities, standard processes for conducting a hunt, and metrics to track success.

Management's Response: NASA Non-Concurs. NASA's position is that this recommendation is not the responsibility of Caltech as a NASA contractor. Once the National Institute of Standards and Technology provides Federal agencies with the appropriate formal, documented threat-hunting guidance to implement, NASA will move forward to establish this capability.

Estimated Completion Date: N/A

Recommendation 9: Develop and implement a comprehensive strategy for institutional information technology (IT) knowledge and incident management that includes the dissemination of lessons learned to system administrators and other appropriate personnel.

Management's Response: NASA Concurs. Caltech indicated that JPL currently conducts year-round cybersecurity awareness presentations to the broader JPL community with a focus on staff with a cybersecurity function (e.g., system administrators). The JPL CISO uses the information from past incidents to help inform the JPL community, as well as create recommendations or modifications for cybersecurity policies and practices. JPL updated the cybersecurity Incident Response Plan (IRP), which provides details for communicating incident findings and lessons learned. JPL will also review the communications plan contained in the IRP to ensure all appropriate personnel receive relevant lessons-learned data. JPL commits to continue sharing incident and vulnerability information with the system administrators and other cybersecurity practitioners as appropriate. The NMO, in coordination with the NASA OCIO, will oversee the execution of the recommendation response.

Estimated Completion Date: September 30, 2019

The OIG also recommends the NASA Chief Information Officer:

Recommendation 10: Include requirements in the pending IT Transition Plan for implementation of continuous monitoring tools that provide the NASA Security Operations Center (SOC) with oversight of JPL network security practices to ensure they adequately protect NASA data, systems, and applications.

Management's Response: NASA Concurs. The overall JPL IT Transition Plan is currently being worked by NASA OCIO, NMO, and Caltech. Draft language addressing this specific action is pending the final approval and signature in the new JPL IT Transition Plan and the Performance Evaluation Management Plan (PEMP).

Estimated Completion Date: September 30, 2019

The Agency reviewed the draft report for information that should not be publicly released. As a result of this review, NASA's position is that the final report, in its entirety, should not be released publicly. A meeting held between the OIG, NASA OCIO, NMO, and JPL on May 17, 2019, resulted in proposed revisions to the draft report that, if accepted by the OIG, would allow the public release of the report.

Once again, thank you for the opportunity to review and comment on the subject draft report. If you have any questions or require additional information regarding this response, please contact Dennis Mahon, NMO, on (818) 393-6779.

Renee P. Wynn
Chief Information Officer

Marcus A. Watkins
Director, NASA Management Office

cc
Jet Propulsion Laboratory/Dr. Watkins

APPENDIX D: REPORT DISTRIBUTION

National Aeronautics and Space Administration

Administrator
Deputy Administrator
Associate Administrator
Chief of Staff
Associate Administrator for Human Exploration and Operations Mission Directorate
Chief Information Officer
Director, NASA Management Office
Director, Jet Propulsion Laboratory
Director, Johnson Space Center

Non-NASA Organizations and Individuals

Office of Management and Budget
    Deputy Associate Director, Energy and Space Programs Division

Government Accountability Office
    Director, Office of Contracting and National Security Acquisitions

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 Aviation and Space

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 Reform
    Subcommittee on Government Operations

House Committee on Science, Space, and Technology
    Subcommittee on Investigations and Oversight
    Subcommittee on Space and Aeronautics

(Assignment No. A-18-012-00)