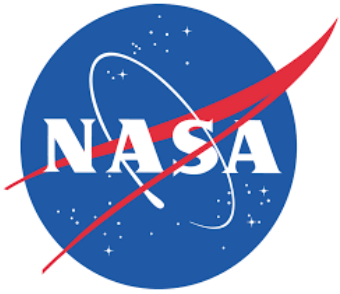


Office of Inspector General

Office of Audits

CYBERSECURITY MANAGEMENT AND OVERSIGHT AT THE JET PROPULSION LABORATORY

June 18, 2019

Report No. IG-19-022

TABLE OF CONTENT

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.

BACKGROUND

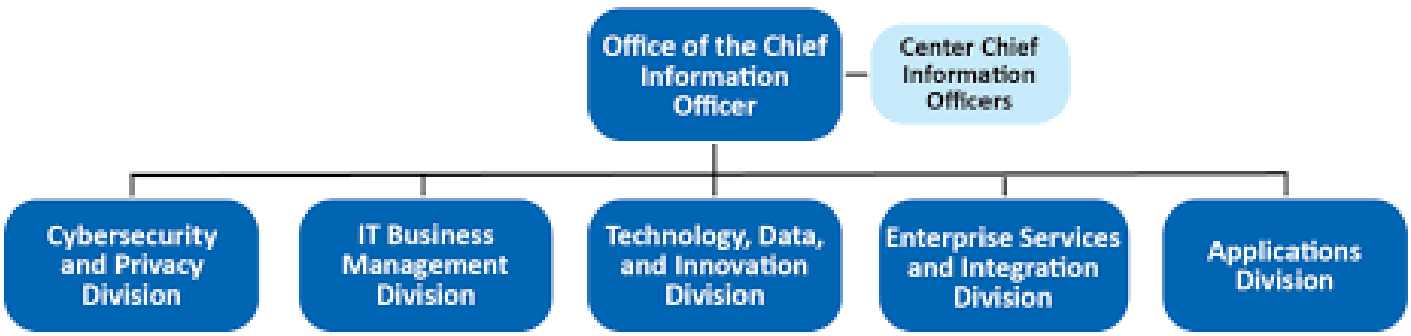
NASA's mission IT network is distributed throughout the United States and hosts hundreds of systems and projects. The Agency's IT portfolio includes systems that control spacecraft, collect and process scientific data, provide security for critical infrastructure, and enable Agency personnel to collaborate 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.

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 Headquartersbased 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.

Figure 1: NASA OCID



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.

Results in Brief

Office of Inspector General

Office of Audits

June 18, 2019

IG-019-22

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 RECOMMEND

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.