

NASA

National Aeronautics and Space Administration

Office of Inspector General

Office of Audits

AUDIT OF NASA'S SECURITY OPERATIONS CENTER

May 23, 2018

Report No. IG-18-020





Office of Inspector General

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

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



RESULTS IN BRIEF

Audit of NASA's Security Operations Center

NASA Office of Inspector General
Office of Audits

May 23, 2018

IG-18-020 (A-17-009-00)

WHY WE PERFORMED THIS REVIEW

NASA spends approximately \$1.4 billion per year on information technology (IT) investments for 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. The Agency also maintains a significant Internet presence with approximately 3,200 publicly accessible websites and web applications that allow NASA to share information on its aeronautics, science, and space programs with the public and worldwide research community. 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.

Managing IT security incidents at NASA is a highly decentralized activity involving the Agency's Headquarters and nine Centers. In November 2008, NASA created the Security Operations Center (SOC) at Ames Research Center (Ames) to identify and respond to Agency-wide security threats to NASA networks and IT systems. The SOC is part of the Office of the Chief Information Officer (OCIO) and is overseen by the OCIO's Senior Agency Information Security Officer (SAISO). The SOC received \$14.7 million in funding for fiscal year 2018, and its services are provided via a task order issued under a much larger IT support contract at Ames. Ten NASA civil service and 36 contractor personnel staff the SOC.

In this review, we assessed NASA's management of the SOC as well as its operations, capabilities, workload, and resource management. To complete this audit, we reviewed Federal and NASA IT security policies as well as industry best practices. We also interviewed NASA Headquarters, Center, and SOC officials and benchmarked with IT officials at the Federal Bureau of Investigation, the Department of Justice's Justice Management Division, and the Department of Energy.

WHAT WE FOUND

Since its inception a decade ago, the SOC has fallen short of its original intent to serve as NASA's cybersecurity nerve center. Due in part to the Agency's failure to develop an effective IT governance structure, the lack of necessary authorities, and frequent turnover in OCIO leadership, these shortcomings have detrimentally affected SOC operations, limiting its ability to coordinate the Agency's IT security oversight and develop new capabilities to address emerging cyber threats. In sum, the SOC lacks the key structural building blocks necessary to effectively meet its IT security responsibilities.

Industry best practice for an effective SOC recommends a charter signed by stakeholders that explicitly details authorities and responsibilities. Such a charter would allow the SOC to more effectively push for the resources and the cooperation required to execute its mission. However, after 10 years the NASA SOC has no charter to govern its operations or outline its authorities. In addition, the SOC has no roadmap for moving from its current state to a future state of operation, a critical management tool for establishing priorities for continual improvement.

Similarly, the SOC lacks authority to manage information security incident detection and remediation for the entirety of NASA's IT infrastructure. Specifically, the SOC does not have operational level agreements (OLA) in place with key divisions, Centers, and Mission Directorates that would allow comprehensive visibility of both institutional and Mission systems – that is, the systems and related networks that support the Agency's aeronautics, science, and space programs. Instead, the SOC relies on informal agreements and personal relationships (with varying degrees of success), resulting in a lack of visibility into Mission networks and high-value IT assets, insufficient ability to store data and determine relationships between potentially suspicious events, incomplete network mapping, and missed opportunities to reduce duplication and leverage economies of scale. Taken together, these shortcomings limit the SOC's capacity to effectively respond to cyberattacks and proactively protect NASA's IT assets.

SOC officials attribute many of the organization's challenges to a lack of leadership stability. In the 10 years since the SOC was established, nine different individuals have served as SAISO or Acting SAISO. Because the SAISO is responsible for managing an Agency-wide information security program and identifying SOC priorities, frequent turnover in this position has resulted in constantly changing priorities and management direction. For example, in 2016 the then-SAISO canceled six projects SOC officials argued were needed to address critical cybersecurity gaps. Less than a year later, funding for four of the projects were reinstated by the OCIO when the SAISO left NASA after serving in the position for about a year. However, the Agency spent \$3.3 million on the two projects that were canceled.

Finally, the current contract vehicle used to procure SOC services limits the Agency's operational flexibility and the ability of SOC management to measure contractor performance. Instead of utilizing a dedicated, Agency-wide service contract, NASA procures SOC services through a task order on a much larger IT services contract at Ames. Because the current SOC task order accounts for only 2.7 percent of the contract's total current award value, any performance issues at the SOC will not significantly affect the contractor's overall performance evaluation, resulting in little ability under the contract to motivate improvement. Additionally, while NASA Headquarters funds the task order for SOC operations, Ames procurement officials are responsible for managing the contract and evaluating contractor performance. Consequently, OCIO's insight and supervisory authority over this critical Agency-wide enterprise has been limited, adversely affecting SOC personnel and resources.

WHAT WE RECOMMENDED

To ensure the SOC is best positioned to serve as the Agency's front line of cyber defense and better monitor, detect, and mitigate cyber incidents across NASA, we made six recommendations: (1) develop a charter and set of authorities that address the SOC's organizational placement, purpose, authority, and responsibilities; (2) establish OLAs with appropriate NASA entities; (3) perform an Agency-wide assessment of storage solutions to support Agency incident detection and response capabilities; (4) develop initiatives to support network mapping to improve the SOC's Agency-wide visibility and enable effective decision making; (5) perform an analysis and document the benefits of either maintaining the current SOC contract structure or transitioning to a dedicated SOC contract to improve performance and flexibility; and (6) identify, utilize, and reduce unnecessary duplication of the incident monitoring, detection, and response capabilities, including toolsets and competencies, available Agency-wide to enhance the capabilities and resources of the SOC and realize efficiencies.

We provided a draft of this report to NASA management who concurred with our recommendations and described planned corrective actions. We consider the proposed actions responsive for five of the six recommendations and will close them upon their completion and verification. With regard to Recommendation 1, the Agency did not specifically indicate whether the SOC charter and authorities would be approved by the NASA Administrator. Therefore, we consider this recommendation 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

Introduction	1
Background	1
NASA’s Security Operations Center Not Well Positioned to Meet Current and Future Needs	10
Ineffective Management Structure.....	10
Structure of Security Operations Center Contract Hinders Operational Flexibility and Performance Oversight	23
SOC Contract Structure	23
Contract Oversight Concerns	24
Contract Adversely Affects Personnel and Resources	25
Conclusion	27
Recommendations, Management’s Response, and Our Evaluation	28
Appendix A: Scope and Methodology	30
Appendix B: Prior SOC Assessments	32
Appendix C: Life-Cycle Activities	33
Appendix D: Management’s Comments	35
Appendix E: Report Distribution	38

Acronyms

ACES	Agency Consolidated End-user Services
ACITS	Ames Consolidated Information Technology Services
APT	Advanced Persistent Threat
CIO	Chief Information Officer
COOP	Continuity of Operations
COR	Contracting Officer Representative
DFAAR	Distributed Forensic Acquisition, Analysis, and Retention
ETDR	End Point Threat Detection and Response
FY	Fiscal Year
GAO	Government Accountability Office
IPS	Intrusion Prevention System
IT	Information Technology
ITIL	Information Technology Infrastructure Library
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OLA	Operational Level Agreement
SAISO	Senior Agency Information Security Officer
SIEM	Security Information and Event Management
SOC	Security Operations Center
WAVE	Web Application Vulnerability Evaluation

INTRODUCTION

NASA spends approximately \$1.4 billion per year on information technology (IT) investments for 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. NASA also maintains a significant Internet presence with approximately 3,200 publicly accessible websites and web applications. Through its websites, the Agency shares information on its aeronautics, science, and space programs with the public and worldwide research community. 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.

In November 2008, in an effort to improve NASA's security posture, the Agency consolidated what had been Center-based computer security incident detection and response programs into a single, Agency-wide entity called the Security Operations Center (SOC). Located at Ames Research Center (Ames), the SOC is NASA's central coordination point for continuous monitoring of computer network traffic entering and leaving NASA facilities. The SOC also includes an information system known as the Incident Management System that coordinates, tracks, and reports on IT security incidents across the Agency.

In this review, we assessed NASA's management of the SOC and its operations, capabilities, workload, and resource management. See Appendix A for details on the audit's scope and methodology.

Background

In a world where IT systems are constantly challenged by more frequent and more sophisticated attacks, it is vital that Federal agencies protect their assets from wide-ranging cybersecurity risks. One such cyberattack occurred in June 2015 when the Office of Personnel Management discovered that sensitive personal information from millions of current, former, and prospective Federal employees and contractors had been stolen from its systems¹. NASA's high profile and its advanced technology make the Agency's computer systems and networks an attractive target for cyber intruders. Over the years, NASA has increasingly become a target of a sophisticated form of cyberattack known as an advanced persistent threat (APT) in which unauthorized individuals seek to steal information rather than cause damage to a network. The individuals or nations behind these APTs are typically well organized and well funded.

The SOC seeks to provide NASA with an enterprise-wide ability to identify and respond to security incidents by monitoring NASA networks and systems, including more than 160,000 confirmed devices used by tens of thousands of civil service employees and contractors. Specifically, the SOC's capabilities include detecting malware on NASA systems, blocking access to malicious websites, collecting and

¹ GAO, "OPM Has Improved Controls, but Further Efforts Are Needed" (GAO-17-614, August 2017).

analyzing cyber intel, and employing multi-layered, cyber-defense mechanisms to identify and prevent malicious events from occurring. In addition, the SOC utilizes tools provided by the Department of Homeland Security to protect against cyberattacks, including the Continuous Diagnostics and Mitigation program and the “Einstein” network sensor program.²

In July 2013, Ames officials awarded a contract valued at up to \$403 million to the Arctic Slope Regional Corporation, Research and Technology Solutions (Arctic Slope) to provide the Center with comprehensive IT support services under what is known as the Ames Consolidated Information Technology Services (ACITS) 3 contract. Funding for the SOC is provided via a task order issued from this contract. As of February 2018, the SOC employed 10 NASA civil servants and 36 contractor personnel.

NASA’s portfolio of IT assets fall into two general categories: (1) “institutional” systems and related networks the Agency uses to support administrative functions such as budgeting, human resources, and email, and (2) “Mission” systems and related networks that support the Agency’s aeronautics, science, and space programs. Examples of the latter include computer systems that support the International Space Station and interplanetary projects such as Juno and the Curiosity Mars rover.

While the SOC’s original intent was to provide end-to-end monitoring, incident detection, and response services for the entirety of NASA’s network and systems footprint, the reality is that a series of challenges prevent the SOC from meeting this enterprise-wide goal. Ten years after its creation, the SOC continues to lack visibility into the majority of NASA’s Mission systems even while it bears significant responsibility for protecting those systems.

SecureInfo Analysis of NASA’s Pre-SOC Incident Management Posture

In 2007, the year before NASA established the SOC at Ames, the Agency hired SecureInfo, an independent cybersecurity consulting firm, to examine the Agency’s then-stratified cyber incident management approach and compare it to a centrally managed, SOC-based approach. SecureInfo reviewed SOC requirements, interviewed key personnel, and conducted site visits to Ames, Goddard Space Flight Center (Goddard), and Marshall Space Flight Center (Marshall). Further, for each of these Centers, SecureInfo evaluated capabilities, performed detailed cost analysis of the total annualized investment and cost of SOC ownership, and prepared a rough order of magnitude for equipment and labor costs to develop a SOC.³ The contractor found that in 2007 NASA had invested approximately \$12 million in annual labor costs for its existing, decentralized incident management approach and that by comparison the Agency would spend \$10.8 million in annual labor costs to operate a centralized SOC after development investments, resulting in approximately \$1.3 million annual savings in labor costs.

² The Continuous Diagnostics and Mitigation program helps identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first. The Einstein system helps protect Federal civilian executive branch agencies by detecting and blocking cyberattacks from compromising agencies and providing the Department of Homeland Security with threat information to help protect the rest of the Federal Government.

³ A rough order of magnitude is an estimate of a project’s potential cost and schedule provided in the early stages when its scope and requirements are not fully defined.

As part of its recommendations on where to locate the SOC facility, SecureInfo estimated total cost of ownership ranging between \$6.9 and \$8.9 million at Goddard (Maryland), \$7 million at Ames (California), and \$4 million at Marshall (Alabama). The analysis noted that Goddard did not have adequate facilities to house a SOC (requiring an additional \$2 to \$4 million to update facilities). Furthermore, the analysis noted that although locating the facility at Ames would require the same number of personnel as Goddard and Marshall, it would require the highest labor rates. In addition, the analysis showed that Marshall's existing incident detection and response operation could be enhanced to meet SOC requirements without additional investment in infrastructure with labor rates the lowest of the three Centers.

The SecureInfo study also provided a three-stage recommendation for developing and operating an Agency-wide SOC: (1) initial operating capability, (2) enhanced operating capabilities, and (3) desired operating capabilities. To achieve initial operating capability, SecureInfo recommended enhancing Marshall's existing 24 hours a day, 7 days a week incident detection operation. For the security monitoring and management components, SecureInfo suggested NASA develop a "virtual SOC infrastructure" that would enable security operations to be performed at any location. SecureInfo noted that in addition to a virtual SOC, NASA should augment Marshall's staff to perform three of four shifts per day with the final shift performed at Ames to take advantage of the time difference between the two Centers.

In January 2008, the Agency's Deputy Chief Information Officer (CIO) for IT Security presented a proposal to the NASA CIO for a distributed SOC model that leveraged existing capabilities from Ames, Goddard, and Marshall.⁴ However, the NASA CIO at the time rejected this recommendation and instead decided to locate the entire SOC at Ames. According to Agency officials, the NASA CIO did not clearly communicate his rationale for this decision.

Office of the Chief Information Officer

The Office of the Chief Information Officer (OCIO) is responsible for NASA's IT governance as well as managing and securing the Agency's IT assets and operations. Authority for developing IT policies and implementing Agency-wide IT programs lies with the Headquarters-based Agency CIO and OCIO staff. In addition to the Headquarters-based Agency CIO and OCIO staff, each NASA Center has a CIO and dedicated IT staff while each Mission Directorate has an IT official with the duties of a CIO. The Agency CIO is responsible for providing leadership, planning, policy direction, and oversight of Agency-wide IT resources. The Agency CIO also serves as the principal advisor to the NASA Administrator and other senior officials on IT matters and is responsible for ensuring NASA acquires and manages its information assets in accordance with Federal policies, procedures, and legislation.

The Headquarters OCIO is organized in four divisions:

- *Capital Planning and Governance* serves as the central policy and business management division within the OCIO. This division is responsible for developing consistent information resources management policies; overseeing the development and promoting the use of information

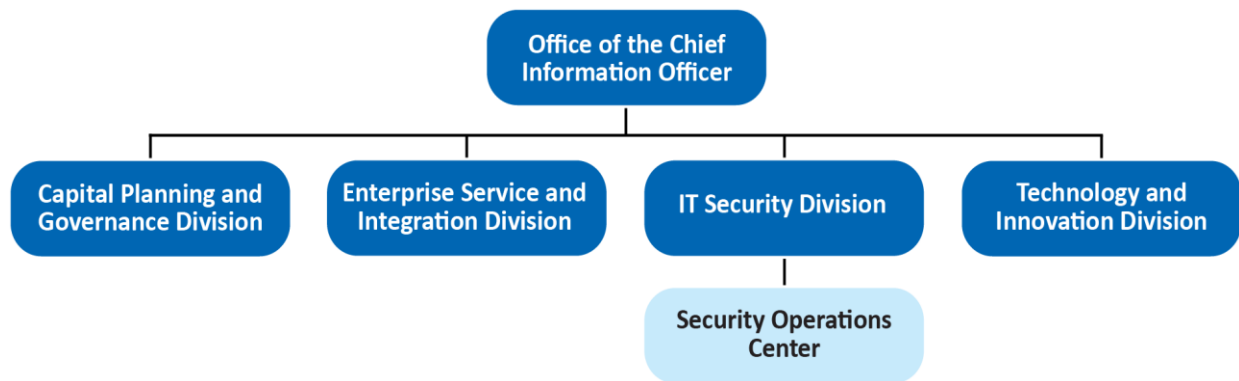
⁴ The recommendation included expanding the existing monitoring capability at Marshall to include enterprise-wide visibility, management, and operation of the NASA SOC. Among other things, Ames would continue to manage advanced incident analysis.

management principles, standards, and guidelines; evaluating Agency information resource management practices to determine their adequacy and efficiency; and determining compliance with OCIO policies, principles, standards, and guidelines.

- *Enterprise Service and Integration* implements NASA’s enterprise architecture.
- *IT Security* manages Agency-wide security projects to correct known vulnerabilities, reduce barriers to cross-Center collaboration, and provide IT security services in support of NASA’s systems and e-Gov initiatives.
- *Technology and Innovation* guides NASA’s IT strategy and investment decisions, identifies emerging IT technologies, and addresses issues such as technology infusion, procurement, and future IT workforce development

Figure 1 illustrates the OCIO organizational structure as of January 2018.

Figure 1: NASA OCIO Organizational Structure



Source: NASA Office of Inspector General (OIG) presentation of NASA Policy Directive 1000.3E, “NASA Organization w/Change 32,” April 15, 2015, information.

Each Federal agency CIO is required to name a Chief Information Security Officer, known at NASA as the Senior Agency Information Security Officer (SAISO). The SAISO oversees the IT Security Division and serves as the principal advisor to the Agency CIO and other NASA officials on information security matters. In addition, the SAISO

- manages the NASA information security program;
- plans for the adoption of new information security technologies throughout the Agency;
- establishes a process for planning, implementing, evaluating, and documenting remedial actions to address deficiencies and weaknesses in NASA’s information security program; and
- ensures NASA develops, disseminates, annually reviews, and appropriately updates policy, procedure, and technical documentation related to information security.

Since the SOC’s establishment in 2008, nine different individuals have served as SAISO, six of whom have served in an “acting” capacity, including the current SAISO.

SOC Organization and NASA Incident Response Process

Incident management at NASA is a highly decentralized activity. NASA stratifies the Agency's incident management response across its Headquarters and nine Centers. The SOC plays a coordination role in monitoring and detecting cybersecurity incidents, with incident management personnel at the SOC and NASA Centers responsible for responding to cybersecurity incidents, including monitoring, detecting, reporting, analyzing, and remediating.

In March 2017, the OCIO issued NASA's Incident Response and Management Handbook (the Handbook), detailing the roles, responsibilities, and processes for employees and contractors in responding to cyber-related incidents, including security incidents involving NASA information assets.⁵ Additionally, the SOC Concept of Operations designates the SOC Operations Manager (a civil servant) as the senior SOC official responsible for the overall operation of the SOC and directs the individual to report to NASA management and communicate with the SAISO and the Ames CIO on IT security concerns.⁶

The SOC is comprised of four operational areas – Monitoring and Detection, Computer Forensic and Incident Analysis, Detection and Integration Services, and Threat and Vulnerability Assessment – that each report to the SOC Operations Manager and provide incident monitoring, detection, response, analysis, and remediation.

The SOC manages incidents through four key steps:

1. opening an event for action after a reported or discovered cyber-related concern;
2. analyzing the event to determine how to respond to, mitigate the effects of, and report the matter;
3. assessing in-depth the event's root cause, review of analogous events, and assessment of its impact; and
4. closing the event and implementing process improvements.

When an information security incident is suspected, it is typically reported to analysts in the SOC's Monitoring and Detection unit via telephone or email, or through the Incident Management System, a centralized database used to report, prioritize, categorize, and track incidents. The Monitoring and Detection group acts as the Agency's IT information security incident handler, facilitating communication regarding the incident between NASA Centers. If the incident appears to be a valid threat, an analyst in the Monitoring and Detection group will investigate. If the analyst is unable to establish whether the incident occurred, they will assign it to the applicable Center Incident Response Team or a Computer Forensic and Incident Analysis analyst, as appropriate, for further investigation. If the analyst is able to confirm the incident, they assign it to the applicable Center for remediation. The SOC's Monitoring and Detection group coordinates any necessary response between parties across the Agency. In the event of a serious enterprise-wide incident, the group will host a teleconference to develop a coordinated Agency response.

⁵ The Handbook covers both cybersecurity events and incidents. Cybersecurity events are any observable occurrences in a system or network such as a user connecting to a file share service, a server receiving a request for a web page, a user sending email, or a firewall blocking a connection attempt. Adverse events result in a negative consequence such as a system crash, unauthorized use of system privileges, unauthorized access to sensitive data, or execution of malware that destroys data. A cybersecurity incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. An information security incident is an adverse event or situation associated with electronic and non-electronic information that poses a threat to the integrity, availability, or confidentiality of that system.

⁶ NASA Security Operations Center, "Concept of Operations" (March 2015).

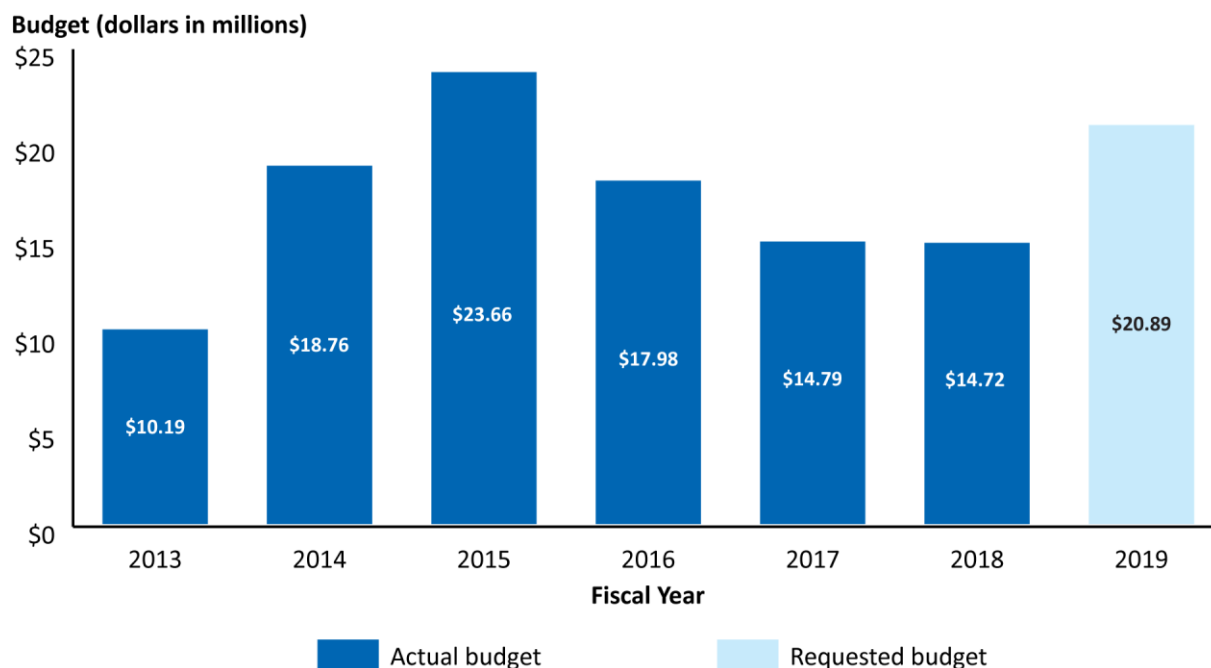
The Handbook further outlines that the Centers, rather than the SOC, provide their own incident monitoring inside their firewalls. At the onset of an incident, the Center activates its Incident Response Team to investigate the issue. For incidents involving Mission systems, the system owner or designated IT security staff will play a key role on the Incident Response Team. While individual Centers may perform mitigation and prevention actions in response to a particular incident, if the SOC determines that these actions need to be performed Agency-wide, it will coordinate a response at the Agency level. The SOC does not perform remediation actions itself but instead relies on Center or Mission Directorate staff who have the authority and capability to block specific internet data.

In 2013, SOC management surveyed the Centers to determine NASA’s overall incident response capabilities. The type of information requested included forensics capabilities, reverse engineering capabilities, training, certifications, malware analysis capabilities, and available IT tools. The SOC hoped to use this information to more efficiently distribute work, reduce duplication, and maximize resource allocation and use of special skills across the Agency. However, the effort was canceled before completion due to a lack of response from the Centers.

SOC Budget

The SOC consistently operates at a level of roughly 5 to 6 percent of OCIO’s overall budget. As shown in Figure 2, from fiscal years (FY) 2013 through 2018, the SOC received approximately \$100 million in total funding, with a high of \$23.66 million in 2015 and a low of \$10.19 million in 2013.⁷ For FY 2019, the SOC has requested \$20.89 million.

Figure 2: SOC Budget



Source: NASA OIG presentation of NASA budget information.

⁷ Funding is through September 30, 2017. Increases in 2014 and 2015 were due to additional funding in the IT Security Division budget to improve the security of NASA’s network. A realignment of funds from the SOC to cover other higher-priority Agency security efforts caused the 2017 reduction.

Prior NASA Office of Inspector General Audits

The NASA Office of Inspector General (OIG) has conducted a substantial body of audit work over the past decade examining the governance, procurement, and security of NASA IT systems. For example, in August 2012 we reported that while the SOC had improved NASA's computer security incident detection and handling capability on the Agency's institutional systems and networks, it did not monitor NASA's Mission networks. This is significant because the bulk of NASA's high- and moderate-impact systems reside within Mission networks. We also found that NASA's computer systems and networks remained at high risk for loss of sensitive data because network firewalls and the SOC's intrusion detection capabilities were ineffective for either preventing or detecting sophisticated APTs. Further, we found NASA was not adequately prepared in the event SOC functionality was lost due to a natural disaster or other major disruption of operations.⁸ While NASA has improved its approach to protecting against APTs and has an ongoing project to ensure SOC continuity of operations, lack of visibility into Mission networks and their high-value assets remains a significant concern.

In a June 2013 audit, we found the decentralized nature of NASA's operations hindered the Agency's ability to implement effective IT governance. In addition, we reported that the Agency CIO operated in an organizational structure that marginalized their authority, and the IT governance structure was overly complex and did not function effectively.⁹ A follow-up audit in October 2017 found the OCIO had made insufficient progress to improve NASA's IT governance since the 2013 report.¹⁰ Specifically, the Agency CIO continues to have limited visibility into IT investments across NASA, the OCIO continues its decade-long struggle to establish an effective enterprise architecture, and the OCIO continues to exercise limited ability to influence IT management within the Centers and Mission Directorates due to the autonomous nature of NASA's field operations.

A July 2014 OIG report found that while NASA's ongoing efforts to reduce its web presence and identify vulnerabilities on its publicly accessible web applications had improved Agency IT security, NASA needed to close remaining security gaps, strengthen program oversight, and further reduce the number of publicly accessible web applications.¹¹

Finally, in a February 2017 report we found that despite its significant presence across the Agency and its criticality to the success of the Agency's Mission, NASA had not adequately defined operational technology, developed a centralized inventory of operational technology systems, or established a standard protocol to protect systems that contain operational technology components. Further, we found that NASA lacked an integrated approach to managing risk associated with its critical infrastructure that incorporates physical and cybersecurity considerations in all phases of risk assessment and remediation.¹²

⁸ NASA OIG, "Review of NASA's Computer Security Incident Detection and Handling Capability" (IG-12-017, August 7, 2012).

⁹ NASA OIG, "NASA's Information Technology Governance" (IG-13-015, June 5, 2013).

¹⁰ NASA OIG, "NASA's Efforts to Improve the Agency's Information Technology Governance" (IG-18-002, October 19, 2017).

¹¹ NASA OIG, "Security of NASA's Publicly Accessible Web Applications" (IG-14-023, July 10, 2014).

¹² NASA OIG, "Audit of Industrial Control System Security within NASA's Critical and Supporting Infrastructure" (IG-17-011, February 8, 2017).

Prior SOC Assessments

Over a 5-year period beginning in November 2010, NASA's IT security environment, including the SOC, was the subject of nine different internal and external assessments. The topics of these assessments ranged from the Agency's cybersecurity risk related to APTs, to the maturity level and performance of the SOC, to an evaluation of NASA's IT security program compared to industry practices. See Appendix B for descriptions of each assessment, including the completion date and objectives.

The assessments identified several recurring themes, including weaknesses in functional management, governance, data storage, continuity of operations (COOP), and cross-functional integration such as a lack of visibility into Mission networks. Eight of the nine assessments made recommendations to address a variety of challenges, which we discuss in more detail later in this report.

The OCIO attempted to initiate another assessment of the SOC in January 2017 and issued a statement of work to an IT consulting firm under an existing NASA contract at Goddard. The assessment was intended to evaluate the SOC's security tools, methodology, security operations, incident response and management, recovery, COOP, and disaster response. However, Ames and SOC personnel expressed concern over the consultant's security clearances, the team's accessibility to the SOC, and the rules of engagement for the assessment. Ultimately, based on disagreements between OCIO, SOC, and Ames officials, the assessment was canceled.

Industry Best Practice

Several nongovernmental entities have developed resources to help organizations design and manage effective SOC operations and related IT security governance.

- *MITRE Corporation.* MITRE Corporation's *Ten Strategies of a World-Class Cybersecurity Operations Center* focuses on improving IT security in the Federal Government.¹³ With respect to SOCs, MITRE emphasizes the importance of several key factors including organizational relationships to a SOC's constituency, distribution of resources, and the authority to meet its obligations to the Agency.
- *ITIL.* Formally the IT Infrastructure Library, ITIL is a set of detailed practices that focus on aligning IT services with the needs of business.¹⁴ Managed by Axelos, an organization that promotes best practice methodologies, ITIL describes processes, procedures, tasks, and checklists that enable organizations to establish a baseline from which they can plan, implement, and measure improvement.
- *SANS Institute.* The SANS Institute is a private for-profit company specializing in information security and cybersecurity training. Topics include cyber and network defenses, incident response, digital forensics, and IT audit. The SANS Institute is a prominent provider of cybersecurity training and certification to professionals, governments, and commercial institutions worldwide.

¹³ Zimmerman, Carson, "Ten Strategies of a World-Class Cybersecurity Operations Center" (Bedford, MA: MITRE, 2014).

¹⁴ AXELOS, "ITIL Continual Service Improvement" [Norwich, UK: TSO (The Stationery Office), 2011].

SOC Activities across the Federal Government

Although NASA’s mission is unique, the challenges the Agency faces in designing and managing an effective SOC are not. As part of this review, we benchmarked with IT officials at the Federal Bureau of Investigation, the Department of Justice’s Justice Management Division, and the Department of Energy to gain insight into their SOC-related efforts. We selected these organizations based on similarities in size, IT architecture, and geographic dispersion relative to NASA.

NASA'S SECURITY OPERATIONS CENTER NOT WELL POSITIONED TO MEET CURRENT AND FUTURE NEEDS

Since its inception a decade ago, the SOC has fallen short of its original goal to serve as NASA's cybersecurity nerve center. Due in part to the Agency's failure to develop an effective IT governance structure coupled with frequent turnover in OCIO leadership, this shortcoming has detrimentally affected SOC operations by limiting its ability to coordinate the Agency's IT security oversight and mature new capabilities for the future. Specifically, we found a lack of clarity in the SOC's oversight authority; undefined relationships between the SOC and functional areas in the OCIO, Centers, and Mission Directorates; and lack of visibility into and data sharing between the SOC and NASA's Mission networks. Taken together, these shortcomings limit the SOC's capacity to respond to cyberattacks and proactively protect NASA's IT assets.

Ineffective Management Structure

Agency policy directs the NASA CIO to allocate resources for an Agency-wide SOC managed by the SAISO to provide centralized, consolidated coordination for information security incident management, response preparation, identification, analysis, communication, containment, eradication, recovery, and follow-up activities. However, structural, procedural, and operational constraints hinder the SOC's ability to meet these responsibilities and limit the likelihood it can develop a more proactive security posture. Specifically, the SOC lacks key structural building blocks to position it to effectively meet these IT security responsibilities. Moreover, our examination of best practices coupled with benchmarking activities with other Federal Government organizations further emphasized the need for these foundational elements.

SOC Lacks a Charter Outlining its Authorities and Responsibilities

The SOC lacks a charter to govern its operations and describe its authorities. MITRE recommends that an effective SOC should have a charter signed by stakeholders that explicitly details its authorities and responsibilities. Armed with such a document, a SOC can more effectively push for the resources and cooperation it needs to execute its mission. Further, according to industry experts, an effective charter can speed resolution of critical issues between parties by specifically identifying decision makers. Similarly, IT officials at other Federal agencies highlighted the importance of a charter as a necessary foundation to achieving a successful, high-performing SOC operation.

In addition to lacking a charter, the SOC has no roadmap or plan for continual service improvement to address its strategic vision or overall goals. Again, SOC officials stated that due to changes in priorities that have occurred due to the continuous turnover in the SAISO position a roadmap for the SOC was never developed. In addition, given that many aspects of IT governance remain an ongoing challenge for NASA, OCIO managers have yet to determine how the SOC fits into the Agency's overall IT security landscape.

ITIL highlights the importance of aligning IT service strategies with the organization's strategic vision to serve as the starting point for agreeing on and establishing priorities for continual improvement of the identified principles. ITIL further states that even though accomplishing the overall strategic vision may be years away, it is necessary to define specific goals to be accomplished within manageable timeframes. As the NASA SOC matures and evolves, it is critical that it develop a roadmap illustrating how it plans to move from its current state to a future state of operation consistent with the OCIO's overall strategic vision. Such a plan can become the starting point to establishing priorities for continual improvement. While NASA IT security officials may not be able to control when an information security incident will occur, they can control how well they are prepared to respond.

Operational Level Agreements, Authority, and Characterization of SOC

To effectively execute its mission, the SOC must have appropriate visibility and access (usually remote) to IT assets that belong to other organizations within NASA and in an environment where the OCIO often has limited authority. Fundamentally, NASA has not established, through Agency policy or other designation, the SOC's authority to manage information security incident detection and remediation oversight for the entirety of NASA's IT infrastructure. In practice, the SOC has access and insight into the Agency's institutional IT networks but not its Mission networks. Specifically, the SOC does not have visibility beyond Mission network firewalls without affirmatively being granted access by Mission IT officials. However, no NASA policies or formal agreements require Mission Directorates to grant the SOC such access. In addition, even if permitted inside, the SOC has no tools designed for analyzing traffic or detecting signature-based threats inside Mission network firewalls.

As discussed in our 2012 audit concerning NASA's incident management capabilities, the Missions largely use suites of IT security tools to perform monitoring, incident detection, and response on their own systems. However, this situation creates the potential for duplication of capabilities and efforts across NASA.¹⁵ At a minimum, the SOC, the Centers, and the Mission Directorates require operational level agreements (OLA) to ensure NASA is properly investing in security and making the most of specialized skillsets. While the SOC has overall responsibility for information security incident monitoring, detection, and prevention, it has little visibility into Mission operations and key assets residing on those networks. Moreover, the SOC and the Mission Directorates lack any formal agreements to ensure, at a minimum, that passive network monitoring, log collection, and analysis is taking place.¹⁶

¹⁵ IG-12-017.

¹⁶ Passive monitoring entails monitoring traffic already on the network.

Further, in lieu of formal written agreements with the Mission Directorates and other internal stakeholders, the SOC relies – with varying degrees of success – on informal agreements and personal relationships in its efforts to share security-related information with these entities. Inevitably, this results in

- a lack of visibility into Mission networks and high-value IT assets,
- insufficient ability to store data and determine relationships between potentially suspicious events,
- incomplete network mapping, and
- missed opportunities to reduce duplication and leverage economies of scale.

To address these issues, IT security best practices suggest the use of OLAs that define the working relationship between different functional areas within an organization. As of November 2017, the SOC had no OLAs with any of the NASA functional areas necessary to achieve its mission.

To be effective, the SOC also needs to routinely interact with numerous Agency offices:

- The *Communications Service Office* manages the Agency's Network Operations Center.
- The *Network Operations Center* is responsible for monitoring the health of NASA's networks.
- The *End User Services Office* manages the Agency Consolidated End-user Services (ACES) contract, which provides email services, computer workstations, and mobile devices to NASA civil servants and contractors.
- The *Web Services Office and Agency Applications Office* provide enterprise architecture and applications portfolio management services.

In addition, the SOC needs to interact with every NASA Center because each is responsible for its IT and communications architecture in addition to hosting Mission Directorate-related projects.

Each of these organizations maintains IT assets and operations to meet individual Agency objectives while the SOC is responsible for protecting the entire Agency from malicious threats. For instance, the End User Services Office is responsible for a large portion of the end user devices including desktops, laptops, and mobile devices deployed throughout the Agency. In addition, the Communications Service Office, Web Services Office, and Agency Applications Office are responsible, respectively, for NASA's networks, websites, and applications portfolio, all of which are additional avenues for attack that could be used to gain unauthorized access to NASA systems and data. The SOC – intended to serve as the nerve center for NASA's cyber incident detection and monitoring – has not been formally integrated into any of these organizations even though it relies heavily on each entity's secure processes and data.

Absent an overarching and detailed charter, OLAs can help address the problem of IT silos by identifying specific criteria to which each functional area must adhere. The criteria would include such topics as standardized processes for incident monitoring, detection, and response; data sharing and storage responsibilities; change management plans; communications management; and technology requirements. The overall objective of an OLA is to present a clear, concise, and measureable description of SOC (and other service providers) internal support relationships and the requirements of the parties under that agreement. Formalizing expectations in an OLA helps ensure roles and responsibilities are clearly described and agreed upon. However, in lieu of OLAs, the SOC operates using ad hoc, personal relationships to address issues as they arise. Without OLAs the SOC may be unable to

respond to an information security incident at a Center without assistance from the local Center whose network is at risk. In a scenario presented by a Center IT official, it is possible that the SOC could identify malicious activity during off-duty hours but could not take steps to stop the attack until appropriate personnel from that Center returned to the office.

NASA's reliance on personal relationships rather than formal procedures for IT decision making is not new. In a 2013 report, we found that Center and Mission Directorate personnel generally did not collaborate through the Agency's formal governance structure but instead Center personnel relied on personal relationships to gain a comfort level with the security posture of Mission Directorate IT assets and make IT-related decisions.¹⁷ In a follow-up report 4 years later, we found the OCIO had made little progress in formalizing its decision-making processes, leaving customers across the Agency operating under the previous inefficient and ineffective framework.¹⁸

Further, officials throughout NASA that we spoke with for this report expressed confusion about the SOC's management and its overall authorities and responsibilities. According to its Project Plan, the SOC was expected to create a consolidated security operations and incident response capability to provide Agency-wide, end-to-end visibility and monitoring of NASA networks and systems. However, our interviews of OCIO and SOC personnel revealed a lack of consensus as to how NASA defines the SOC and its related responsibilities and authorities. While some officials thought of the SOC as a service, another classified it as an Agency program.¹⁹

An appropriate classification of the SOC ensures that it is aligned with an appropriate organizational placement and receives commensurate authorities within the Agency. NASA Interim Directive 7120.99 defines programs and activities as follows:

- *Program* – a strategic investment by a Mission Directorate or Mission Support Office that has a defined architecture and/or technical approach, requirements, funding level, and a management structure that initiates and directs one or more projects. A program defines a strategic direction that the Agency has identified as needed to implement Agency goals and objectives.
- *Activity* – an operation that sustains NASA as an organization. Unlike projects, which are temporary and unique, activities are ongoing and repetitive.²⁰

We found that the SOC is not managed as an activity or a program. While the SOC does not implicitly meet the definition of a service, program, or activity, establishing the appropriate organizational placement and related authority for the SOC is crucial to enabling effective performance. Moreover, according to an OCIO official involved in NASA IT governance, the issue of the SOC's role is not part of Agency IT governance discussions.

This lack of clarity regarding the SOC's authority and responsibility is further complicated by its odd supervisory structure. At the time of our fieldwork, the SOC Operations Manager – the senior SOC official – reported to an individual within the Ames OCIO rather than the Agency SAISO. This creates a

¹⁷ IG-13-015.

¹⁸ IG-18-002.

¹⁹ ITIL defines a service as “a means of delivering value to customers by facilitating outcomes customers want to achieve without the ownership of specific costs and risks.”

²⁰ NASA Interim Directive 7120.99, “NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements,” December 22, 2011.

reporting structure in which the SAISO has operational authority over the enterprise-wide SOC, but does not supervise the official in charge of SOC operations. This reporting structure – apart from creating, at times, an uncomfortable dynamic between Ames and Headquarters IT officials – directly contradicts language in NASA Procedural Requirements (NPR) 2810.1A, which states that the SAISO is responsible for SOC operations.²¹ In a January 2018 memorandum, the OCIO stated that as part of on-going improvements to NASA’s cybersecurity program, it was developing a plan to implement an Enterprise Security Service Office that will affect “the structure of the security services provided by the SOC.”²² As a part of this plan, the OCIO redefined the SOC Operations Manager as the SOC Program Executive and made the position a direct report to the SAISO while creating a SOC Operations Lead to manage SOC personnel and handle day-to-day operations reporting directly to an Ames IT official. We are unclear as to the impact of this change, and question whether this reporting structure will result in greater SAISO authority and visibility into SOC operations.

Limited Visibility into Mission Network and High-Value Assets

NASA’s Mission networks support spaceflight programs, ground stations, and vital Mission essential infrastructure. However, since its establishment the SOC has had limited visibility into or, in many cases, knowledge of critical Mission Directorate IT assets. While NPR 2810 creates an Agency-wide SOC, neither that directive nor any other directive specifically requires Missions to share data or information about their networks with the SOC. Over the years, OCIO officials have attempted to improve their visibility through initiatives to identify high-value assets and establish informal relationships and information sharing between the SOC and Mission Directorates. However, in most cases the responsibility for network and asset protection remains entirely with the Missions, with the SOC playing no role in assessing and detecting threats. With no knowledge of specific applications, operating systems, or other device information, the SOC is severely limited in its ability to assist the Missions or to correlate event data across institutional and Mission network boundaries when an information security incident occurs. Since its formation 10 years ago, the SOC’s visibility into Mission Directorate systems has been hobbled by distributed organizations, unclear network boundaries, confusion about the architecture of NASA’s institutional network, and a lack of formal agreements with Mission Directorates to share information.²³

MITRE and the SANS Institute suggest that visibility into system data and networks is key to understanding how systems and networks are connected, monitoring their network traffic activity, and prioritizing SOC resources and capabilities based on risk across the architecture. Such comprehensive visibility would allow the SOC over time to learn what type of network activity is normal and what may be anomalous, enabling it to take more of a risk-based approach to monitoring, detection, prevention, and response that in turn would help prioritize IT security resources. MITRE also suggests that the degree of visibility normally available varies depending on a SOC’s organizational model and the size of its constituency. In NASA’s case, greater visibility into Mission networks would allow for increased situational awareness and improved collaboration and information sharing, leading to an enhanced Agency security posture.

²¹ NPR 2810.1A, “Security of Information Technology,” May 16, 2006.

²² NASA OIG, “NASA’s Contract Vehicle for Security Operations Center Services (A-17-009-00)” (November 15, 2017).

²³ NASA institutional systems support the day-to-day work of NASA employees and include networks, data centers, Web services, desktop and laptop computers, enterprise business applications, and other end-user tools such as email and calendaring.

Need for Improved Logging, Data Storage, and Correlation

The SOC does not have access to critical logs and other IT security information, hindering its ability to correlate data to identify similarities and relationships.²⁴ In addition, NASA does not have a policy that identifies which devices or software should capture logs, the types of logs that should be captured, or the amount of time these logs should be retained. Logging information is a critical piece of evidence to determine whether a security event actually occurred and, if so, provide details to assist in mitigating and preventing future similar events. Comparing logs from a variety of sources helps to reconstruct the chain of events of an incident or anomalous activity. For example, the SOC does not have access to “Active Directory” logs on NASA’s institutional networks or intrusion detection system alert logs, firewall logs, full session network packet capture, NetFlow, and security logs on the Mission networks.²⁵ These limitations on SOC access stem from challenges with NASA’s network architecture, institutional and Mission network boundaries, and a lack of horizontal integration across the functional areas. Each of these data sources currently unavailable to SOC personnel could provide them valuable information when analyzing cyber events, including log in and authentication sources, time stamps, and source and destination internet protocol addresses. Lack of access to necessary data logs coupled with limited visibility into Mission Directorate systems and networks limits the SOC’s ability to identify the root cause of an incident. For example, reviewing the appropriate logs and correlating data across multiple sources can help the SOC determine the exact location where an incident occurred, when it occurred, the source or external actor responsible for the incident, and if there was any lateral movement through the network – information critical for both a criminal investigation and mitigating the breach’s impact.

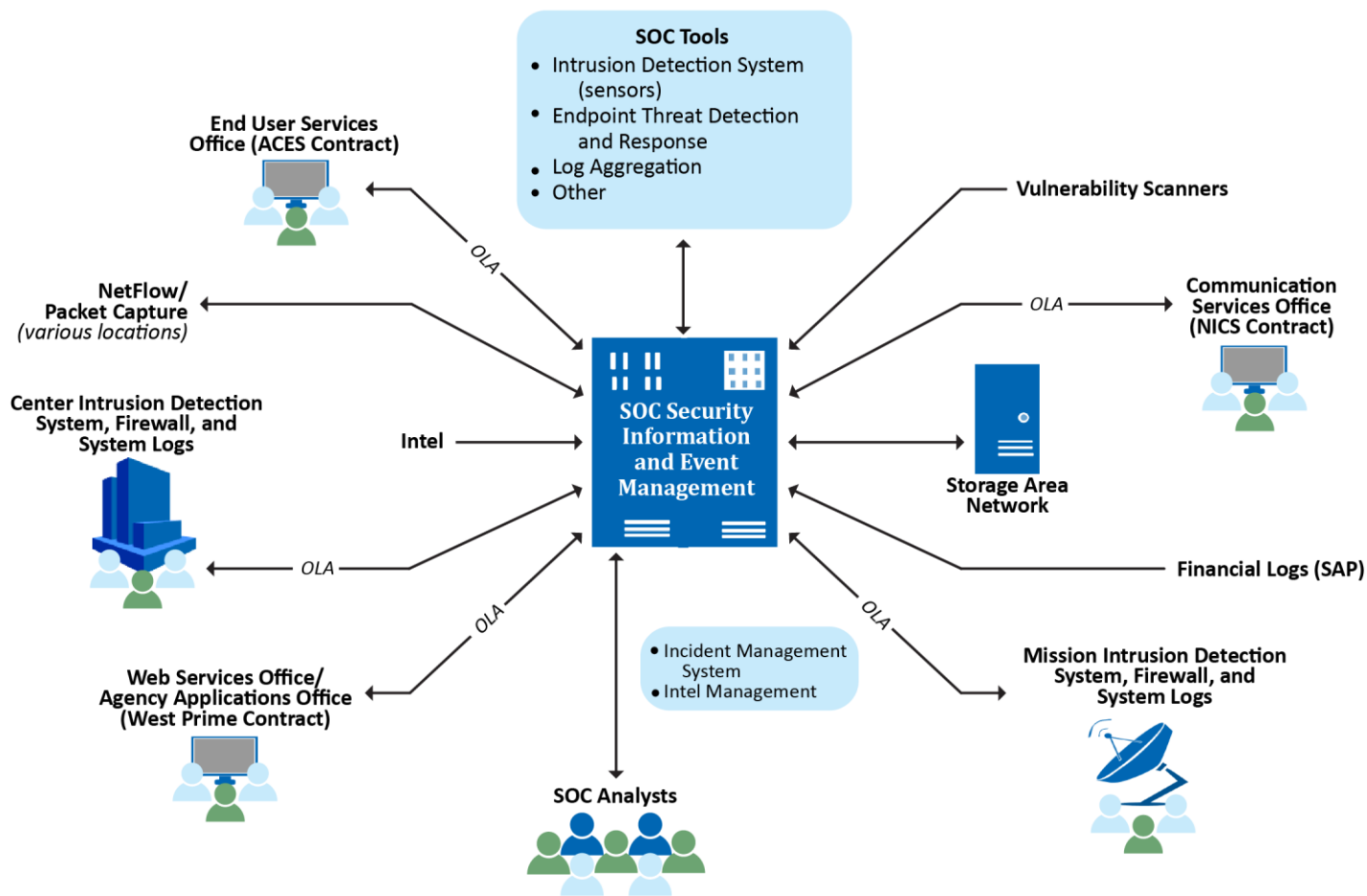
Given the extremely large volume of data that flows across NASA networks and systems daily, adequate IT storage capacity is essential to enable the SOC to maintain necessary levels of historical data for analysis and remediation, particularly when a security incident is not immediately detected and may spread to other locations prior to detection. The SOC’s data storage capacity for its Security Information and Event Management (SIEM) platform reached full capacity at 12 terabytes as of October 2017 and the SOC Operations Manager informed us that the capacity needs to increase to at least 25 terabytes to meet future requirements.²⁶ Figure 3 presents a graphical representation of the SOC’s need for visibility, logging, data access, and storage capacity.

²⁴ Logging is the process of collecting and storing audit, security, and event data over time.

²⁵ Active Directory is a directory service Microsoft developed for Windows domain networks included in most Windows Server operating systems. A server running Active Directory is called a domain controller and authenticates and authorizes all users in a Windows domain network – that is, assigning and enforcing security policies for all computers and installing or updating software. Full packet capture creates a copy of network traffic data for future analysis or investigative activity. NetFlow is a network protocol for collecting Internet protocol traffic information and monitoring network traffic.

²⁶ The Security Information and Event Management platform provides real-time analysis of security alerts generated by network hardware and applications. This platform enables an analyst to quickly identify suspicious occurrences in the systems and determine if an event has occurred by quickly correlating large amounts of data.

Figure 3: SOC Workflows and Data Requirements



Source: NASA OIG representation of possible enterprise SIEM implementation.

Incomplete Network Mapping

NASA has not developed a complete network map of its enterprise architecture to identify the physical connectivity of all Agency networks and devices.²⁷ Therefore, the Agency does not have a comprehensive awareness of its physical and logical IT footprint. For instance, a SOC system analyst would have difficulty determining the physical location of a system where an anomalous event is occurring without a reliable map of the Agency’s network. Moreover, such a map would enable the SOC to identify where high-value assets reside and make better management decisions to allocate resources based on risk.

²⁷ A network map is a visualization of devices on a network, their inter-relationships, and the transport layers providing network services.

Absent a complete network map, the SOC is only able to gather mapping data through a time-consuming manual process. The lack of complete network mapping coupled with the SOC's lack of visibility into Mission networks means the SOC is unable to identify and protect many critical assets in the NASA architecture because they do not know they exist. Despite this shortcoming, the NASA OCIO has not allocated resources to remedy the situation due to constantly changing priorities and a lack of OLAs among the SOC, Communications Services Office (which has responsibility for mapping initiatives), and the Mission Directorates.

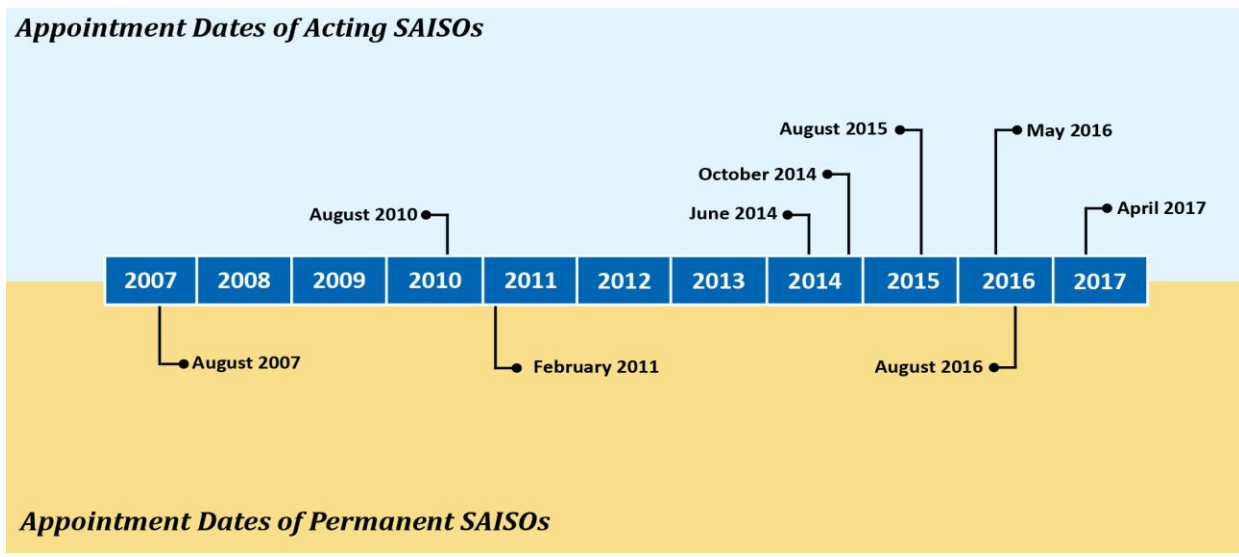
MITRE and the SANS Institute both cite the importance of mapping data for effective SOC oversight. MITRE further suggests that a SOC should be able to obtain network-mapping data through a combination of automatic and manual processes and that this mapping should take place at least annually to ensure timely recording of network changes. As previously mentioned, NASA's lack of formal OLAs between the SOC, Communications Services Office, End User Services Office, Web Services Office, Agency Applications Office, Mission Directorates, and Centers results in a lack of visibility into much of the Agency's enterprise architecture. In addition to identifying several other elements that should be included in the OLAs, best practice supports maintaining a reliable map of the Agency's networks.

According to SOC personnel, commercially available automated network mapping products would provide valuable additional information related to the connectivity of high-value assets to NASA's network. Knowing this would enable the SOC to prioritize resources using risk-based metrics. Further, a robust mapping capability would enhance the SOC's ability to understand normal versus abnormal network traffic, essential to identifying and preventing security incidents. In 2015, the SAISO at the time planned to invest \$1.8 million in a commercial mapping product. However, shortly thereafter the SAISO left the Agency and his successor decided not to move forward with the mapping investment citing differing priorities. In lieu of adoption of an Agency-wide network mapping solution, three NASA organizations external to the OCIO each purchased the same product through separate procurements at a total cost of approximately \$800,000. Therefore, the Agency spent approximately 40 percent of the cost previously determined to address the Agency's enterprise-wide mapping needs on mapping efforts for three individual NASA organizations.

High Turnover in SAISO Position Results in Changing Priorities

In the 10 years since the SOC was established, nine different individuals have occupied the SAISO position. Of those nine different individuals, only three were appointed permanently to the position while the rest held the role in an "acting" capacity. SOC officials said they face challenges addressing operational issues and technical gaps given the changing priorities of whomever occupies the SAISO position at any given time. Figure 4 depicts the turnover of the SAISO position since creation of the SOC.

Figure 4: Appointment Dates of SAISOs Since SOC Inception



Source: OIG analysis of OCIO-provided data.

In a previous report, we noted high turnover of senior IT managers, including the SAISO, had negatively impacted NASA’s IT operations, affected the Agency’s ability to execute its IT governance structure, and hindered the Agency’s ability to significantly improve NASA’s IT security posture.²⁸ Because the SAISO is responsible for managing an Agency-wide information security program and identifying SOC priorities, frequent turnover in this position has resulted in constantly changing priorities and management direction. In addition, SOC managers repeatedly mentioned the frequent turnover in the SAISO position as a factor in their inability to gain approval and funding to resolve long-standing technical issues. The ongoing and unresolved challenges identified during the following assessments demonstrate the effects of the lack of stable leadership on the SOC.

Prior SOC Assessments Highlight Impact of Changing Leadership

The SOC’s performance and NASA’s IT security environment have been the subjects of multiple internal and external reviews. Over a 5-year period beginning in November 2010, NASA and several outside entities completed nine assessments of either the SOC or NASA’s overall IT security environment.²⁹ Each of the nine assessments identified challenges with the SOC or NASA’s approach to IT security. We categorized the issues, challenges, or gaps identified in each assessment as follows:

- *Functional management* includes the business aspects of operating the SOC, such as contract management, program implementation, formulation and execution of budgets, and monitoring and reporting of financial and workforce resources.
- *IT governance* are the processes that ensure effective and efficient use of IT resources and provides the structure for integration of those resources across an organization.

²⁸ IG-18-002.

²⁹ Appendix B lists the authors, dates of completion, and objectives of each assessment.

- *Storage area networks* are specialized, high-speed networks that provide network access to storage. Storage area networks are typically composed of hosts, switches, storage elements, and storage devices that are interconnected using a variety of technologies, topologies, and protocols. Storage area networks are often used to improve application availability, enhance application performance, increase storage utilization and effectiveness, and improve data protection and security.
- *Continuity of operations (COOP) plans* ensure redundancy of operations.
- *Cross-functional integration* aligns cross-functional interdependencies through interaction, information sharing, and collaboration.

Table 1 describes the challenges identified in each assessment and whether the assessment made recommendations to mitigate the issues identified.

Table 1: Challenges Identified in Prior SOC and IT Security Assessments

Assessment Title	Date Completed	SOC Specific	Functional Management				IT Governance	Cross-Functional Integration ^b	Storage Area Network (SAN)	COOP	Recommendations Made to Mitigate Issues
			Staffing	Budget	Management Turnover	SOC Contract					
<i>Northrop: NASA Cyber Security Vulnerability Assessment</i>	November 2010	No	X					X	X		X
<i>NASA SOC Assessment</i>	August 2011	Yes	X	X	X	X	X			X	X
<i>Verizon: NASA SOC Assessment Performance and Maturity Level Observations</i>	May 2012	Yes	X	X		X	X	X	X	X	X
<i>Dell: Code I Efficiencies</i>	September 2013	No	X		X	X		X			X
<i>Whyte SOC Observations</i>	March 2014	Yes				X	X				
<i>Gartner: Current State Baseline IT Environment</i>	September 2014	No	X				X			X	X
<i>NASA IT Security Portfolio</i>	2014 ^a	No	X					X		X	X
<i>NASA SOC Challenges and Opportunities</i>	November 2015	Yes	X		X		X	X			X
<i>Enterprise IT Security Tiger Team Assessment</i>	December 2015	No	X		X		X	X			X
Total Assessments			8	2	4	4	6	6	2	4	8

Source: NASA OIG analysis of SOC and NASA IT security assessments.

^a The assessment began in 2014 and the completion date is unknown.

^b Includes visibility of Mission networks.

All nine assessments identified management challenges, including lack of staff resources, supervisory turnover, and the structure of the SOC contract. Further, the assessment findings demonstrate that many of the identified issues continue to occur. For example, an internal NASA assessment completed in August 2011 noted a lack of prioritization of SOC requirements and identified management turnover as a threat to SOC operations, both of which remain issues today.

Additionally, six of the nine assessments identified cross-functional integration and governance as challenges. In November 2010, Northrop noted NASA had decentralized security monitoring under multiple network segments and recommended the Agency empower a single information security organization with operational authority over all Agency networks.

Four of the assessments identified the lack of a COOP plan as an issue for both the SOC and the Agency. Two internal and two external assessments specifically noted the SOC had not established a COOP plan and recommended development of a SOC-wide business continuity, disaster recovery, and contingency plan. Additionally, in our August 2012 report we found NASA was not adequately prepared for the potential loss of the SOC due to a natural disaster or other major incident given the absence of a backup capability.³⁰ We recommended the CIO develop procedures for transferring incident detection responsibility to NASA Centers in the event of a SOC disruption. In response to this recommendation, the OCIO is in the process of establishing a SOC COOP site to centralize incident detection responsibility in the event of a disruption. As of March 2018, the recommendation remained open.

In total, eight of the nine assessments made recommendations to address a variety of issues but in only one instance did NASA management indicate it agreed with the recommendation. In a December 2015 assessment, a NASA IT Security Tiger Team recommended several options for aligning the IT security responsibility within the OCIO and the Agency's IT Management Board noted its agreement with one of the options.³¹ During the course of our current review, we attempted to determine mitigation actions taken in response to the assessments. According to a NASA official, informal responses were provided and mitigation was attempted but addressing the issues has been difficult due to continuous management turnover.

Cancellation and Reinstatement of SOC Projects

In August 2016, SOC personnel briefed the newly appointed Agency SAISO on seven projects to enhance SOC and Agency cybersecurity capabilities, several of which NASA IT security officials deemed critical to SOC operations. Each project was in a development phase ranging from formulation (beginning stages) to implementation.³² The projects ranged from a SOC Lifecycle Refresh Project – an effort that would upgrade IT infrastructure – to a Web Application Vulnerability Evaluation to assess the vulnerability of NASA websites.

Subsequent to the briefing, the SAISO canceled six of the seven projects – projects on which the Agency already spent approximately \$15 million up to that point. Table 2 describes the six canceled projects, four of which were ultimately reinstated in 2017 by the OCIO when the permanent SAISO left NASA after serving about a year.

³⁰ IG-12-017.

³¹ The NASA Information Technology Management Board consists of the Agency CIO, the Deputy and Associate CIOs, the Center CIOs, and the Mission Directorate CIOs, and makes decisions regarding the Agency's IT infrastructure strategy, operations, and budget.

³² See Appendix C for a description of NASA project life-cycle phases.

Table 2: SOC Projects Canceled in 2017

Project	Description	Ensuing Life-Cycle Phase at Cancellation ^a	Funds Expended at Time of Cancellation	Reinstated
COOP	A COOP plan ensures operational redundancies if SOC capabilities are compromised or lost. Loss of all SOC capabilities at Ames would result in a cybersecurity service outage for the entire Agency, meaning NASA would lose the ability to effectively monitor its IT environment and detect and prevent cyber incidents. Without a COOP, reconstituting SOC technical services at another site would take months.	Critical Design Review	\$3.4 million	Yes
SOC Lifecycle Refresh Project	The SOC continues to run servers purchased in 2008 even though the average service “lifespan” for this equipment is 3 years. This project would have replaced obsolete servers. Failure of these servers would result in extended downtime for the SOC and potential loss of critical data.	Test Readiness Review	\$3.3 million	Yes
Distributed Forensic Acquisition, Analysis and Retention (DFAAR)	The DFAAR project was an enterprise solution that would enable SOC staff and subject matter experts to perform timely and collaborative advanced digital forensics on remote IT security incidents.	Test Readiness Review	\$2.8 million	No
Web Application Vulnerability Evaluation (WAVE)	The WAVE project was created to assess the vulnerability of NASA websites and scan the Agency’s web applications to identify, validate, and provide mitigation for vulnerabilities prior to exploitation by malicious third parties.	System Concept Review/System Requirements Review	\$502,000	No
Intrusion Prevention System (IPS)	The IPS project seeks to prevent external, hostile actors from accessing NASA networks by blocking malicious traffic on its web applications.	Key Decision Point-E	\$5.2 million	Yes
Endpoint Threat Detection and Response (ETDR)	The ETDR project seeks to enhance NASA’s ability to conduct remote, forensic data analysis on systems suspected of being compromised, automate live response incident data collection, and scan for known indicators of compromise on a large number of host systems.	Operations Readiness Review	\$0	Yes

Source: NASA OIG analysis of SOC documentation.

^a Life-cycle phases are defined in Appendix C of this report.

The former SAISO told us she canceled the projects because of concerns they did not meet what she considered to be the Agency’s highest IT security priorities and due to concerns about insufficient tracking of project funds. For example, the SAISO acknowledged that while the SOC lacked a forensic analysis capability, the projects being proposed by the SOC would not enable real-time analysis of forensic information. Similarly, due to concerns over the expenditure of funds, the SAISO canceled the COOP project.

At the same time the former SAISO canceled the six IT projects in 2016, she directed SOC managers to seek her approval for all acquisitions and procurements regardless of amount. In addition, in August 2016, due to her dissatisfaction with the level of budget and project spending detail provided by the SOC, the SAISO asked Headquarters budget personnel to assist the SOC in developing a more detailed spending plan to establish a higher level of budget visibility.

SOC officials said they disagreed with the SAISO's actions, arguing the canceled projects were intended to address critical cybersecurity gaps and were essential for maintaining the Agency's cybersecurity posture. In addition, managers said the reasons for cancellation were not adequately communicated to them by the SAISO. In the months following the SAISO's departure in April 2017, the OCIO reinstated funding for four of the six projects – COOP, SOC lifecycle refresh, IPS, and ETDR:

- Due to new project requirements, the SOC reevaluated the cost and schedule for COOP and the project is scheduled to receive \$2.6 million during FYs 2017 through 2019. In October 2017, the CIO chose Johnson Space Center as the COOP location for the SOC, with an anticipated completion date for the project of July 2018.
- The SOC Lifecycle Refresh Project received \$120,000 in additional funding through August 2017, and as of September 2017 merged the remaining funds into SOC operations.
- IPS was completed in April 2017 and is now operational.
- The ETDR operational readiness review was scheduled for November 2017 with implementation expected by May 2018.

While funding for four of the six projects was reinstated, the Agency spent \$3.3 million on the two remaining projects before they were canceled – DFAAR and WAVE.

STRUCTURE OF SECURITY OPERATIONS CENTER CONTRACT HINDERS OPERATIONAL FLEXIBILITY AND PERFORMANCE OVERSIGHT

The current contract vehicle used to procure SOC services limits the Agency's operational flexibility and the ability of SOC management to measure contractor performance. Instead of utilizing a dedicated, Agency-wide service contract, NASA procures SOC services through a task order on a much larger contract for IT services at Ames. Because the current SOC task order accounts for 2.7 percent of the larger contract's total current award value, any SOC performance issues will not significantly affect the contractor's overall performance evaluation, resulting in little ability under the contract to motivate improvement. Additionally, while NASA Headquarters funds the task order for SOC operations, Ames procurement officials are responsible for managing the contract and evaluating contractor performance. Furthermore, even though the Agency's SAISO has ultimate authority over NASA's IT security operations, the SOC Operations Manager at the time of our audit did not report to the SAISO but rather to an Ames IT official. Consequently, the OCIO's insight and supervisory authority over this critical Agency-wide enterprise has been limited, adversely affecting SOC personnel and resources.

SOC Contract Structure

In July 2013, Ames awarded a contract to Arctic Slope for assistance in the following areas: IT systems and governance, IT security, network and communication systems, application management, innovation and emerging technologies, and informational systems. Ames developed the award as an indefinite-delivery, indefinite-quantity contract with firm-fixed-price and cost-plus-fixed-fee task orders at a total value not to exceed \$403.4 million.³³ The contract – known as ACITS-3 – expires in September 2018.

The current task order for SOC operations was awarded for \$8.7 million and has a period of performance from October 1, 2017, through August 31, 2018. The scope of work for the task order includes monitoring and detection, computer forensics and incident analysis, threat and vulnerability assessment, detection and integration services, systems management and network security, technology development, and communications and planning. Ten NASA civil service personnel work alongside 36 contractor employees to provide SOC services.³⁴ The SOC task order is 1 of 29 issued from the larger ACITS-3 contract in FY 2018.

³³ An indefinite-delivery, indefinite-quantity contract provides for an indefinite quantity of services over a fixed period of time. This type of contract is used when an agency cannot determine the precise quantities of supplies or services the Government will require during the contract period. Awards are usually for base plus option years and the Government places task orders against the base contract for individual requirements. A firm-fixed-price contract provides for a price that is not subject to adjustment based on the contractor's cost experience in performing the contract. A cost-plus-fixed-fee contract is a cost-reimbursement contract that provides for payment to the contractor of a negotiated fee fixed at the inception of the contract.

³⁴ Arctic Slope Regional Corporation is the prime contractor while NTT Data and Mandiant Consulting are the SOC subcontractors.

Anticipating expiration of the ACITS-3 contract, in April 2017 Ames procurement officials solicited information from potential parties interested in competing for ACITS-4, the follow-on contract that closely mirrors ACITS-3 requirements. The Agency interviewed interested parties beginning in July 2017 and anticipates awarding the contract prior to September 2018 with SOC services expected to continue as a task order under ACITS-4.³⁵

Contract Oversight Concerns

Within the OCIO, the SAISO oversees the IT Security Division that manages NASA's IT security program in which the SOC plays a prominent role. Typically, under such a structure a SOC Operations Manager would report to the SAISO. However, even though the SOC task order is funded by NASA OCIO, the SOC Operations Manager at the time of our audit reported to an Ames IT Division Chief rather than the SAISO, leaving the OCIO with little formal operational control over day-to-day SOC operations.

The ACITS-3 Contracting Officer Representative (COR) initially told us that the SOC Operations Manager provided performance evaluation input that was factored into the prime contractor's overall performance evaluation. However, the ACITS-3 COR subsequently clarified that the Contracting Officer and the COR are not required to survey entities such as the SOC and its Operations Manager who receive services through task orders about contractor performance. Instead, the SOC Operations Manager – the NASA civil servant in charge of SOC operations – told us he handles contractor performance matters on an informal, "issue-by-issue" basis and does not provide formal input to the ACITS-3 COR about the performance of SOC contractor employees.

The Federal Acquisition Regulation requires evaluations of contractor performance at least annually. These evaluations generally review the entity, division, or unit that performed the contract or service. The Contracting Officer may require performance evaluations for each order in excess of \$150,000 when such evaluations would produce more useful performance information for source selection officials than that contained in the overall contract. Based on the \$8.7 million value of the current year's SOC task order, we believe the SOC Contracting Officer should have required performance evaluations to be completed.

With no formal evaluation of the task order, NASA has not established a record of the contractor's performance and has little leverage through the contract to induce improvement. Moreover, because the SOC task order is such a small percentage of the total value of the ACITS-3 contract, any performance assessment provided by the SOC Operations Manager would not impact the prime contractor's overall rating.

Finally, according to the SOC Operations Manager a subcontractor representative is responsible for the execution of all task work and oversight of prime and subcontractor staff. The subcontractor representative does not provide the SOC Operations Manager formal feedback on prime and subcontractor performance. According to the Federal Acquisition Regulation, the prime contractor retains legal and management responsibility for overall contract performance, which includes managing subcontractor performance. In our view, this relationship should be reviewed to ensure the prime contractor is retaining responsibility for assessing performance of the subcontractors.

³⁵ According to the Contracting Officer, the current plan is to award ACITS-4 before the current contract expires. However, this is subject to change based on the release of the final request for proposal, bid evaluations, and any potential bid protests.

Contract Adversely Affects Personnel and Resources

In 2012, at NASA's request, a private consulting firm conducted an assessment of the SOC that included review of the SOC task order under what was then the ACITS-2 contract.³⁶ Among other things, the assessment found the contract adversely affected the SOC's personnel and resource availability. Specifically, the study noted the following weaknesses:

- The contract in place was not appropriate for an Agency-wide SOC.
- Government involvement was contractually restricted and limited contractor resources available to the SOC.
- SOC funding, budgeting, and contracting resources were proportional to localized project-level scope versus an Agency-wide scope.
- The SOC had no SOC-specific contracting vehicles and instead was funded by task orders on Ames contracts, which introduced limitations that significantly impacted SOC operations including telework mandates, lack of certification requirements, and performance evaluations/actions.
- While the SOC had been able to maximize available contracting resources, the resources were stretched to capacity.
- Procurement for SOC services using an Ames contract resulted in little NASA SOC contractual oversight.

The assessment defined a mature SOC as having resources proportional to Mission scope procured on a SOC-controlled and -dedicated contract vehicle. Such an arrangement would provide the SOC, and ultimately the Agency, operational flexibility and control over this critical cybersecurity resource.

In May 2015, NASA completed a business services assessment of the Agency's IT security program and found it lacked an enterprise-wide risk management framework. In order to facilitate the assessment's goal of establishing an Agency IT security risk management framework, NASA formed a "tiger team" of experts from OCIO and Center security organizations to assess security functions within the IT Security Division, the Enterprise Service and Integration Division, and NASA Centers. The tiger team recommended NASA pursue an integrated IT security service delivery model that aligns with Agency and industry best practice, optimizes security service delivery, and obtains efficiencies across all enterprise service delivery areas. During this review, NASA officials reiterated the value of an enterprise-wide approach to IT security similar to its Agency-wide approach for other IT services such as ACES that provides computer and communications services to NASA employees and contractors. In January 2018, OCIO officials indicated they plan to implement an Enterprise Security Service Office, including the establishment of enterprise-level contracts, to support the delivery of a suite of standard security services across the Agency to include the SOC.

³⁶ Verizon Federal Professional Consulting Services, "NASA SOC Assessment: Performance and Maturity Level Observations" (May 25, 2012).

The SOC provides critical IT security service to NASA Headquarters, Centers, and associated Agency facilities. We believe the current contract structure does not facilitate the optimal level of oversight for such a vital enterprise-wide component of NASA's IT security infrastructure. Due to the impending expiration of the current Ames IT contract in September 2018, we previously communicated our concerns regarding the structure of the SOC contract to the NASA Acting Administrator, Acting Deputy Administrator, and CIO in a November 2017 memorandum. On January 11, 2018, the Agency CIO responded to our memorandum stating the OCIO is developing a plan to implement an Enterprise Security Service Office to include establishment of enterprise-level contracts to support the delivery of standard security services across the Agency. In her response the CIO also indicated future management and contract requirements would be considered in conjunction with the OIG's concerns, although it was not clear how or in what timeframe. We continue to believe the Agency should assess whether awarding a separate, Agency-wide contract for SOC services would provide the SOC, the SAISO, and ultimately the Agency CIO more flexibility to enhance the SOC's operational capabilities to achieve mission goals.

CONCLUSION

NASA's networks and communications systems are under constant threat from hackers and malware, making the response to information security incidents an increasingly complex challenge. An effective Agency-wide SOC should have insight over and access to all equipment and data connected to NASA's systems to mount an effective defense and mitigate cyberattacks. However, the effectiveness of NASA's SOC has been limited by a lack of clarity in its oversight authority; undefined relationships between different functional areas within the OCIO, Centers, and Mission Directorates; and its current contract structure. To maximize its effectiveness, the SOC must position itself with clearly defined objectives, authorities, responsibilities, and enterprise relationships.

RECOMMENDATIONS, MANAGEMENT'S RESPONSE, AND OUR EVALUATION

To ensure the SOC is best positioned to serve as the Agency's front line of cyber defense and better monitor, detect, and mitigate cyber incidents across NASA, we made the following recommendations:

1. The Agency CIO develop a charter and set of authorities signed by the NASA constituent executives (including the NASA Administrator) that addresses the SOC's organizational placement, purpose, authority, and responsibilities.
2. The Agency CIO, in conjunction with the SAISO, establish Operational Level Agreements with NASA Centers, Mission Directorates, the Communications Services Office, the End User Services Office, the Agency Applications Office, and Web Services Office to clearly define incident response roles and responsibilities, ensure data storage and sharing needs are addressed, and opportunities to leverage economies of scale are identified and acted upon in support of Agency cybersecurity goals. The agreements should include (but not be limited to) the following issues:
 - a. responsibilities of signing parties;
 - b. data visibility, sharing, storage, and logging requirements;
 - c. change management plan;
 - d. communications plan;
 - e. an explanation detailing the technology deployments necessary to support the agreement; and
 - f. service levels expected detailing the service benefit to both parties in line with Agency goals.
3. The Agency CIO, in conjunction with the SAISO and OCIO service offices, perform an Agency-wide assessment of storage solutions to support Agency incident detection and response capabilities.
4. The Agency CIO, in conjunction with the Communications Services Office, develop initiatives to support mapping the enterprise network, including Mission Directorate systems beyond institutional boundaries, to improve the SOC's Agency-wide visibility and enhance effective decision making.
5. The SAISO perform and document an analysis of maintaining the current SOC contract structure or transitioning to a dedicated SOC contract to improve performance and flexibility.
6. The Agency CIO identify and reduce unnecessary duplication of the incident monitoring, detection, and response capabilities, including toolsets and competencies available Agency-wide to enhance the capabilities and resources of the SOC and realize efficiencies in the management of these capabilities.

We provided a draft of this report to NASA management who concurred with our recommendations and described planned corrective actions. We consider the proposed actions responsive for five of the six recommendations and will close them upon verification and completion of those actions. With regard to Recommendation 1, NASA management stated that a charter addressing the SOC's organizational placement, purpose, authority, and responsibility will be developed and presented to SOC stakeholders and reviewed and approved by senior OCIO representatives. However, in its response, NASA did not specifically indicate whether the SOC charter and set of authorities would be approved by the NASA Administrator. As NASA's top decision maker, the Administrator aligns the Agency's strategic and policy direction with the interests and requirements of its stakeholders and constituent groups. Given the SOC's critical role within NASA, it is essential the Administrator approve the charter. Therefore, we consider this recommendation unresolved pending further discussion with the Agency.

Management's comments are reproduced in Appendix D. Technical comments have been incorporated, as appropriate.

Major contributors to this report include Laura Nicolosi, Mission Support Director; Scott Riggerbach, Project Manager; Sarah Beckwith; Chris Reeves; and Sarah McGrath.

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



Paul K. Martin
Inspector General

APPENDIX A: SCOPE AND METHODOLOGY

We performed this audit from March 2017 through April 2018 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.

We initiated our review of the SOC to evaluate NASA's management of the organization. Specifically, we evaluated capability, workload, and resource management as well as continuity of operations in line with the SOC's mission and the Agency's cybersecurity posture.

We reviewed Federal and NASA policies as well as industry best practice standards to determine adequate criteria and standards that were applicable to NASA's management and operation of the SOC. The documents we reviewed included the following:

- Office of Management and Budget Memorandum M-11-29, "Chief Information Officer Authorities," August 8, 2011
- National Institute of Standards and Technology Special Publication 800-61 Revision 2, "Computer Security Incident Handling Guide," August 2012
- NPR 2810.1A, "Security of IT," May 16, 2006
- NASA Policy Directive 2810.1E, "NASA Information Security Policy," July 14, 2015
- NASA Interim Directive 7120.99, "NASA IT and Institutional Infrastructure Program and Project Management Requirements," December 2011
- NASA ITS-HBK-2810.09-02A, "NASA Information Security Incident Management Handbook," March 17, 2017
- MITRE's "Ten Strategies of a World-Class Cybersecurity Operations Center," Carson Zimmerman, 2014

We interviewed NASA Headquarters, Center, and SOC officials concerning the management and operation of the SOC. In addition, we benchmarked with IT officials at the Federal Bureau of Investigation, the Department of Justice's Justice Management Division, and the Department of Energy to gain insight into lessons learned and industry best practices. We also reviewed contract documentation as well as various internal and external studies concerning SOC operations.

Use of Computer-Processed Data

The computer-processed data used in this audit did not materially affect the findings and therefore, we did not test the reliability and validity of the data.

Review of Internal Controls

We reviewed Federal regulations and NASA policies and procedures to determine the necessary and established internal controls over SOC operations. We analyzed the execution of the policy

requirements as it related to the internal control structure and concluded that the internal controls were generally adequate except in specific circumstances, as discussed in the body of this report. Our recommendations, if implemented, should correct the weaknesses identified.

Prior Coverage

During the last 5 years, the NASA Office of Inspector General (OIG) and the Government Accountability Office (GAO) have issued 14 reports of significant relevance to the subject of this report. Unrestricted reports can be accessed at <http://oig.nasa.gov/audits/reports/FY18> and <http://www.gao.gov>, respectively.

NASA Office of Inspector General

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

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

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

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

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

NASA's IT Governance (IG-13-015, June 5, 2013)

Review of NASA's Computer Security Incident Detection and Handling Capability (IG-12-017, August 7, 2012)

Government Accountability Office

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

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

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 Cyber Incident Response Practices (GAO-14-354, April 30, 2014)

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

Cybersecurity: A Better Defined and Implemented National Strategy is Needed to Address Persistent Challenges (GAO-13-462T, March 7, 2013)

Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented (GAO-13-187, February 14, 2013)

APPENDIX B: PRIOR SOC ASSESSMENTS

Over a 5-year period beginning in November 2010, nine assessments have been completed on the SOC or NASA's IT security environment. The assessments were completed by both internal and external parties and identified issues and challenges related to IT security at NASA. Assessment objectives varied and included areas such as NASA's cybersecurity risk related to APTs, the maturity level of the SOC, and an analysis of challenges and opportunities associated with establishing an Agency IT security risk management framework. The assessment titles, dates of completion, and objectives are described in Table 3.

Table 3: Objectives and Date of Completion for Prior SOC Assessments

Assessment (Internal/External Entity)	Date Completed	Objectives
Northrop: NASA Cyber Security Vulnerability Assessment (External)	November 2010	To assess NASA's cybersecurity risk related to APTs
NASA SOC Assessment (Internal)	August 2011	To assess the effectiveness and efficiency of the NASA SOC
Verizon: NASA SOC Assessment Performance and Maturity Level Observations (External)	May 2012	To provide NASA with a maturity level and performance assessment of the SOC
Dell: Code I Efficiency (External)	September 2013	To cite opportunities to improve efficiencies across Ames, which includes the SOC
SOC Observations (Internal)	March 2014	To provide observations related to NASA's SOC
Gartner: Current State Baseline IT Environment (External)	September 2014	To evaluate their NASA's IT security program against industry practices and standards, Gartner conducted an assessment of security and risk management in the IT area of NASA OCIO, addressing people, policies, technologies, and overall approach
NASA IT Security Portfolio (Internal)	n/a ^a	Review NASA's IT security portfolio and make observations related to the management and operation of IT across NASA
NASA SOC Challenges and Opportunities (Internal)	November 2015	An OCIO Information Technology Security Division representative created a detailed overview of the challenges and opportunities facing the SOC
Enterprise IT Security Tiger Team Assessment (Internal)	December 2015	To analyze and develop options to address the challenges and opportunities in establishing an Agency IT Security risk management framework and IT security infrastructure that aligns with NASA's business risks

Source: NASA OIG presentation of NASA internal and external assessment data.

^a The assessment began in 2014; however, the completion date is unknown.

APPENDIX C: LIFE-CYCLE ACTIVITIES

NPR 7120.99 establishes the framework by which NASA formulates and executes IT and institutional infrastructure programs and projects. NASA's IT and institutional infrastructure program and project management process is based on life cycles with key decision points. Program life cycles are divided into two phases: formulation and implementation. Formulation consists of Phases A (concept development) and B (preliminary design). Implementation includes Phases C through F beginning with development and resulting in decommission of the project. Assessment activities occur throughout these phases and are described in Table 4.

Table 4: Assessment Activities and Corresponding Life-Cycle Phase

Activity	Description
Formulation Phase	
Key Decision Point Phases A and B	Decision authority determines whether and how the program or project proceeds into the next lifecycle phase and approves any additional actions.
System Concept Review	Evaluates the scope, cost benefit analysis, and a recommended solution/concept for the product or service to be delivered for the purpose of receiving approval, formalized via the Formulation Authorization Document, to proceed to the Formulation Phase. Assesses the effect on the enterprise architecture and ensures applicable security controls are considered.
System Requirements Review	Examines the functional, technical, performance, and security requirements for the system; and elements of the preliminary project plan and ensures that the requirements and the selected concept will satisfy the system objectives.
Preliminary Design Review	Demonstrates that the preliminary design meets all system requirements with acceptable risk and within the cost and schedule constraints and establishes the basis for proceeding with detailed design.
Implementation Phase	
Key Decision Point Phases C through F	Decision authority determines whether and how the program or project proceeds into the next lifecycle phase and approves any additional actions.
Critical Design Review	Confirms that the maturity of the design is appropriate to support proceeding with implementation, that it was developed in conjunction with stakeholders, demonstrates that the design meets detailed requirements, and identifies open design issues for the purpose of obtaining a decision to proceed with development and deployment. It reviews the technical architecture to ascertain the effect on the enterprise architecture and reviews the application security design and the inclusion of security controls.
Test Readiness Review	Evaluates the projects readiness to proceed with testing, ensuring adequate schedule, resources, and management processes are in place. It ensures the completion of an integration test plan and the system's readiness for execution of integration testing
Operational Readiness Review	Determines that the project is ready to go-live with the system or service; that requirements have been met; the functionality, performance, and security controls have been thoroughly tested; procedures are in place for operations; and that the organization responsible for operations and sustaining engineering is ready to assume responsibility. It ensures a security plan is in place and that system authorization has been received.

Project Completion Review	Provides assurance that the implemented system is performing as expected and that all necessary support requirements are in place and functioning properly. It confirms that the system is operating properly in its production environment. It is the official closeout of the project and project team.
Decommissioning Review	Confirms the decision to terminate or decommission the system and assesses the readiness of the system for the safe decommissioning and disposal of system assets.

Source: NASA Procedural Requirement 7120.99, "NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements" (December 22, 2011).

APPENDIX D: MANAGEMENT'S COMMENTS

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



MAY 11 2018

Reply to Attn of: Office of the Chief Information Officer

TO: Assistant Inspector General for Audits
 FROM: Chief Information Officer
 SUBJECT: Agency Response to OIG Draft Report, "Audit of NASA's Security Operations Center" (A-17-009-00)

NASA appreciates the opportunity to review and comment on the Office of Inspector General (OIG) draft report entitled, "Audit of NASA's Security Operations Center" (A-17-009-00), dated April 19, 2018.

In the draft report, the OIG makes six recommendations addressed to the Chief Information Officer (CIO) intended to ensure the Security Operations Center (SOC) is best positioned to serve as the Agency's front line of cyber defense and better monitor, detect, and mitigate cyber incidents across NASA.

Specifically, the OIG recommends the following:

Recommendation 1: The Agency CIO develop a charter and set of authorities signed by the NASA constituent executives (including the NASA Administrator) that addresses the SOC's organizational placement, purpose, authority, and responsibilities.

Management's Response: Concur. The Office of the Chief Information Officer (OCIO) will develop a charter for the (SOC) that addresses the SOC's organizational placement, purpose, authority, and responsibility within the OCIO's CyberSecurity and Privacy Division. The OCIO will present the charter to SOC stakeholders for review and concurrence by the Agency Information Technology Council (ITC) and the NASA Senior Agency Information Security Officer (SAISO) for final NASA CIO approval and signature.

Estimated Completion Date: September 28, 2018.

Recommendation 2: The Agency CIO, in conjunction with the SAISO, establish Operational Level Agreements with NASA Centers, Mission Directorates, the Communications Services Office, the End User Services Office, the Agency

Applications Office, and Web Services Office to clearly define incident response roles and responsibilities, ensure data storage and sharing needs are addressed, and opportunities to leverage economies of scale are identified and acted upon in support of Agency cybersecurity goals. The agreements should include (but not be limited to) the following issues: (a) responsibilities of signing parties; (b) data visibility, sharing, storage, and logging requirements; (c) change management plan; (d) communications plan; (e) an explanation detailing the technology deployments necessary to support the agreement; and (f) service levels expected detailing the service benefit to both parties in line with Agency goals.

Management's Response: Concur. The NASA SOC will work with the OCIO Information Technology (IT) Business Management Division to determine the governance for establishing or updating appropriate Operational Level Agreements. The NASA SOC will also update the existing Service Level Agreements between the SOC and: (1) the Communications Services Office; (2) the Computer Service Program Office; and (3) Center CIO Offices, converting the Service Level Agreements to Operational Level Agreements.

Estimated Completion Date: January 18, 2019.

Recommendation 3: The Agency CIO, in conjunction with the SAISO and OCIO service offices, perform an Agency-wide assessment of storage solutions to support Agency incident detection and response capabilities.

Management's Response: Concur. The OCIO will establish requirements for storage solutions, in support of data logging, data analytics, and data correlation for incident detection and response capabilities. The OCIO will assess the current data storage capabilities across the Agency, in order to determine the gaps required to meet the storage requirements.

Estimated Completion Date: September 28, 2018.

Recommendation 4: The Agency CIO, in conjunction with the Communications Services Office, develop initiatives to support mapping the enterprise network, including Mission Directorate systems beyond institutional boundaries, to improve the SOC's Agency-wide visibility and enhance effective decision making.

Management's Response: Concur. The OCIO is currently implementing an automated tool to map OCIO-managed corporate enterprise networks by the Communications Service Program (CSP). The OCIO will develop initiatives for mapping the entire NASA network infrastructure to improve the SOC's Agency-wide visibility and enhance effective decision making.

Estimated Completion Date: September 16, 2019.

Recommendation 5: The SAISO perform and document an analysis of maintaining the current SOC contract structure or transitioning to a dedicated SOC contract to improve performance and flexibility.

Management's Response: Concur. The Agency CIO, in conjunction with the SAISO, will direct an assessment of the current contract structure under the Ames Consolidated Information Technology Services (ACITS)-3 contract. The assessment results will then be used by the CIO to evaluate maintaining the current SOC contract structure or transitioning to a dedicated SOC contract.

Estimated Completion Date: March 31, 2019.

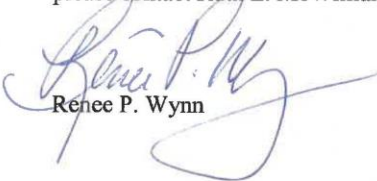
Recommendation 6: The Agency CIO identify and reduce unnecessary duplication of the incident monitoring, detection, and response capabilities, including toolsets and competencies available Agency-wide to enhance the capabilities and resources of the SOC and realize efficiencies in the management of these capabilities.

Management's Response: Concur. The OCIO will identify the incident monitoring, detection, and response services across the Agency. The SAISO will document and assess duplication of services and provide a recommendation to the Agency CIO for targeted implementation in FY20.

Estimated Completion Date: June 28, 2019.

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

Once again, thank you for the opportunity to review and comment on the subject draft report. If you have any questions or require additional information regarding this response, please contact Ruth L. McWilliams on (202) 358-5125.



Renee P. Wynn

APPENDIX E: REPORT DISTRIBUTION

National Aeronautics and Space Administration

Administrator
Associate Administrator
Chief of Staff
Chief Information Officer
Senior Agency Information Security Officer

Non-NASA Organizations and Individuals

Office of Management and Budget
Deputy Associate Director, Energy and Space Programs Division
Government Accountability Office
Director, Office of Acquisition and Sourcing Management

Congressional Committees and Subcommittees, Chairman and Ranking Member

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

(Assignment No. A-17-009-00)