NASA

National Aeronautics and Space Administration

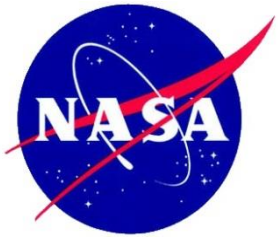
Office of Inspector General

Office of Audits

INDUSTRIAL CONTROL SYSTEM SECURITY WITHIN NASA'S CRITICAL AND SUPPORTING INFRASTRUCTURE

February 8, 2017

Report No. IG-17-011



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.

NASA Office of Inspector General
Office of Audits

RESULTS IN BRIEF

Industrial Control System Security within NASA's Critical and Supporting Infrastructure

February 8, 2017 IG-17-011 (A-16-001-00)

WHY WE PERFORMED THIS AUDIT

In keeping with the evolution of technology, NASA has increasingly moved away from isolated, manually controlled operational technology (OT) systems to an environment in which physical processes are controlled with sophisticated and interconnected information technology (IT) equipment. As more devices become "smart" through wireless connectivity, OT systems that once required hands-on manipulation such as adjusting a valve or flipping a switch can now be controlled remotely. Many of these OT systems are part of the Agency's critical infrastructure used to test rocket propulsion systems, control and communicate with spacecraft, and operate ground support facilities, or are associated with the electrical power, heating and cooling systems, and other supporting infrastructure. While the convergence of IT and OT can lead to cost savings and other efficiencies, it also means OT systems are potentially vulnerable to the types of security challenges more common to IT systems, including malicious hacking.

In this review, we examined whether NASA has implemented effective policies, procedures, and controls to protect the systems it uses to operate its critical infrastructure. To complete this work, we examined NASA's critical infrastructure listing, systems inventory, IT security database, procedural requirements, and documented industry best practices. We also conducted interviews with key NASA personnel and partner agency subject matter experts.

WHAT WE FOUND

Despite its significant presence across the Agency and its criticality to the success of the Agency's multi-faceted mission, NASA has not adequately defined OT, developed a centralized inventory of OT systems, or established a standard protocol to protect systems that contain OT components. NASA needs to know which systems incorporate OT components because applying traditional IT security practices to OT systems can cause the underlying systems to malfunction. For example, a security patch caused monitoring equipment in a large engineering oven to stop running, resulting in a fire that destroyed spacecraft hardware inside the oven. The computer reboot caused by the software upgrade also impeded alarm activation, leaving the fire undetected for 3.5 hours before it was discovered. Further, limited awareness of OT systems across the Agency has led to systems lacking the application of comprehensive security best practices. Moreover, NASA's current policies do not distinguish OT from IT, and the Agency does not offer training focused on protecting OT systems. As a result, NASA is not well-positioned to meet the security demands of an evolving OT environment and is assuming unnecessary risk for critical Agency systems and facilities with OT components.

NASA also lacks an integrated approach to managing risk associated with its critical infrastructure that incorporates physical and cyber security considerations in all phases of risk assessment and remediation. Specifically, the security of physical and cyber components of NASA's critical assets is managed with minimal collaboration among key Agency stakeholders and does not involve the Office of Strategic Infrastructure, which manages the supporting infrastructure associated with critical assets. This disjointed approach has led to duplication of effort and gaps in security planning and risk remediation at both the Agency and Center levels. Further, based on the inconsistent security practices we

observed at various Centers, we question the overall efficacy of NASA's process for identifying critical infrastructure. Finally, inadequate guidance and oversight, coupled with insufficient funding and record keeping, limit the visibility and insight into NASA's critical infrastructure protection processes and ultimately impair the Agency's ability to protect its vital assets.

WHAT WE RECOMMENDED

To ensure the Agency is adequately assessing risk for, applying security controls to, and identifying its critical assets, we made six recommendations: (1) develop a framework to coordinate security efforts across the Agency, (2) develop a standardized process to assess Agency cyber and physical assets for NASA critical infrastructure, (3) ensure appropriate Agency personnel are included in functional reviews of NASA's critical infrastructure assets and facility security assessments, (4) coordinate the development of a methodology for the identification and protection of interdependencies, (5) develop security policy and procedures for managing the protection of OT that addresses key areas identified during this review, and (6) establish an integrated cyber and physical risk management committee or oversight body to ensure NASA is adequately identifying critical infrastructure and supporting interdependencies and appropriately protecting its OT systems.

We provided a draft of this report to NASA management who concurred or partially concurred with our recommendations and described corrective actions the Agency has taken or will take to address them. For recommendations 2 through 5, the Agency partially concurred, pointing to the recent implementation of the Enterprise Protection Program (EPP), which the Agency says will focus on protecting critical capabilities and technologies. However, the response describes the EPP and associated board as advisory in nature. Given the governance concerns we highlighted in this and other reports, we encourage NASA to ensure EPP leadership has sufficient technical authority and support from other responsible components to direct the change required to meet the intent of our recommendations. We believe given the proper authority, EPP can implement appropriate corrective action. Accordingly, our recommendations are resolved and will be closed upon completion and verification of the proposed corrective actions.

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

TABLE OF CONTENTS

Acronyms

CDM	Continuous Diagnostics and Mitigation
DHS	Department of Homeland Security
EPP	Enterprise Protection Program
HVAC	Heating, Ventilation, and Air Conditioning
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
IT	Information Technology
NIST	National Institute of Standards and Technology
NPR	NASA Procedural Requirements
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OPS	Office of Protective Services
OSI	Office of Strategic Infrastructure
OT	Operational Technology
PPD	Presidential Policy Directive
SP	Special Publication

INTRODUCTION

In today's society, information technology (IT) systems play an integral role in the operation of such vital public facilities as power plants, airports, dams, energy pipelines, and transportation systems. Increasingly, one of these roles is to monitor and control the performance of devices like valves and pumps that help run these systems. In the past, these operational technology (OT) systems were controlled by physical or simple electronic manipulation – that is, manually adjusting a valve or activating a switch – and were not connected to or controlled through an IT network. However, as more devices become "smart" through wireless connectivity or other means, OT systems that once required hands-on manipulation can now be monitored and controlled remotely. While this convergence of IT and OT can lead to cost savings and other operational efficiencies, it also means OT systems have become more complex and potentially vulnerable to similar types of security challenges as IT systems, including intentional hacking by actors with malicious motives.

Reflecting the trend in society at large, NASA has also increasingly moved away from isolated, manually controlled OT systems to an environment in which physical processes are controlled with sophisticated IT equipment. Many of these OT systems are part of critical assets the Agency uses to test rocket propulsion systems, control and communicate with spacecraft, and operate ground support facilities. Others are associated with infrastructure supporting these systems like electrical power, gas lines, and heating and cooling systems.

In this review, we examined whether NASA has implemented effective policies, procedures, and controls to protect the systems used to operate its critical infrastructure. See Appendix A for details of the audit's scope and methodology.

Background

Since 2009, the U.S. Department of Homeland Security (DHS) has issued alerts and advisories about suspicious cyber activity, incidents, and vulnerabilities affecting critical infrastructure monitored and controlled by industrial control systems. A subset of OT, industrial control systems are combinations of electrical, mechanical, hydraulic, or pneumatic components that act together to achieve an objective – for example, transporting electricity from a substation to a building.[1] In the past, industrial control systems were generally not connected to IT networks and did not contain complex computing capabilities; therefore, they could be adequately protected using physical security measures like locks and fences. However, as OT has become more integrated with IT, such physical measures are becoming less adequate in securing the underlying critical assets.

For network-enabled control systems, targeted malware can change command outputs and cause various types of malfunctions – for example, motors spinning at dangerously high rates, cooling systems shutting down, liquid or gas valves opening or closing, switches turning off, or electrical components

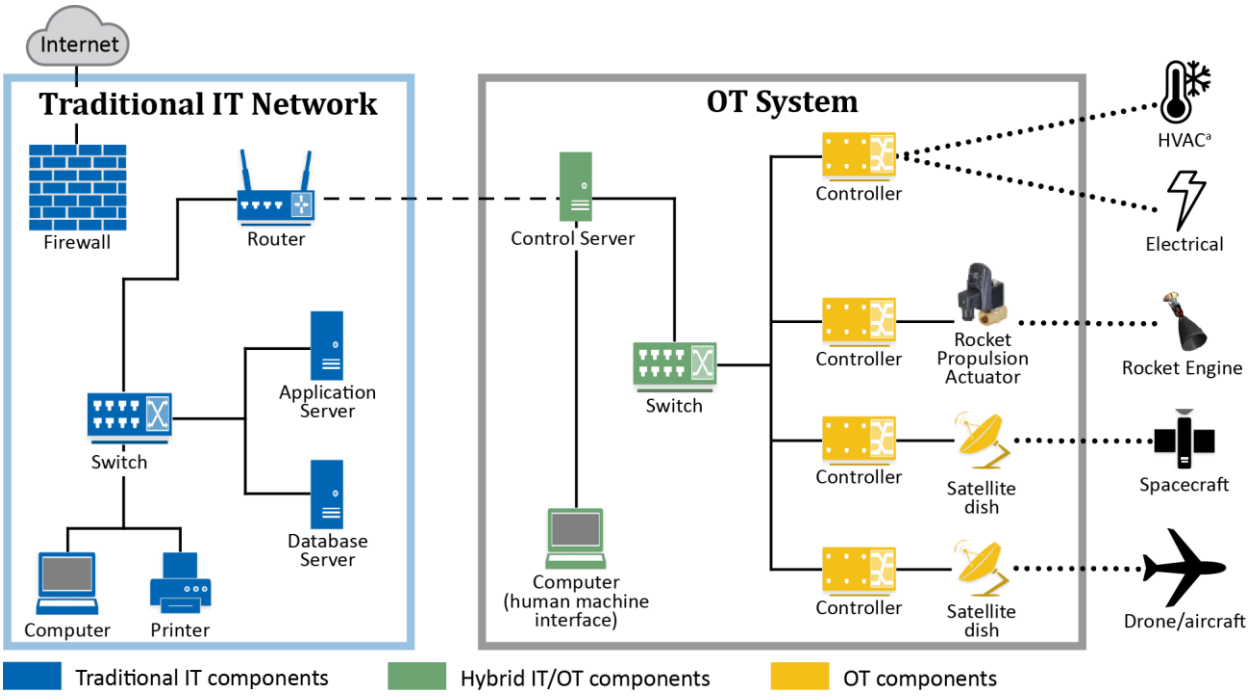
[1] National Institute of Standards and Technology Special Publication (SP) 800-82, Revision 2, "Guide to Industrial Control System Security," May 2015.

overloading. Indeed, even OT systems not connected to larger networks can be affected by IT-related threats if, for example, malware is introduced through an infected USB storage device (thumb drive) or other removable media.[2]

The convergence of IT and OT presents several unique security challenges. First, security solutions designed for IT systems may not be immediately transferable to the OT environment. Many legacy OT system components use small processors with limited computing capabilities, making it difficult to run even basic malware protection software or other security applications. Second, because OT systems often control sensitive physical processes like cooling and heating that must operate continuously, great care must be taken to minimize operational disruptions when applying security controls designed for IT systems. Third, OT systems often utilize specialized, proprietary software that have vulnerabilities that cannot be identified using traditional IT security tools. Finally, OT components tend to have long life cycles, which means embedded software may continue to operate long after the manufacturer has stopped providing support.

At NASA, control OT and hybrid IT/OT systems include environmental monitoring and control systems (e.g., systems that control heating, cooling, ventilation, and power), rocket propulsion testing systems, and spacecraft and aircraft command and control systems. Indeed, as much as 65 percent of the Agency's critical infrastructure is managed and supported by OT systems. Figure 1 illustrates the range of IT and OT assets at NASA that support missions and associated institutional infrastructure.

Figure 1: Illustration of IT/OT Systems at NASA



Source: NASA Office of Inspector General analysis of Industrial Control Systems Cyber Emergency Response Team and NASA-provided documentation.

[a] Heating, Ventilation, and Air Conditioning.

[2] Examples of malware that have affected control systems include Stuxnet, a malicious worm that caused an Iranian nuclear plant to fail by making centrifuges spin much faster than normal, and BlackEnergy, which caused power outages across three regions in Western Ukraine.

National Policy and Guidance for Protection of Operational Technology Systems

The National Institute of Standards and Technology (NIST) has issued guidance applicable or related to industrial control system security. Although NASA has adopted NIST-based guidance that addresses overall IT security, the Agency has yet to incorporate NIST guidance on industrial control system security into its procedures.

NIST Guide and Risk Management Framework for Federal Information Systems

In June 2014, NIST updated the Risk Management Framework (the Framework) for Federal information systems and the guidelines agencies use to apply the Framework.[3] The Framework seeks to improve information security, strengthen risk management processes, and encourage the sharing of resources and procedures among Federal agencies. Specifically, it emphasizes

1. building information security capabilities into Federal information systems through application of state of the practice management, operational, and technical security controls;

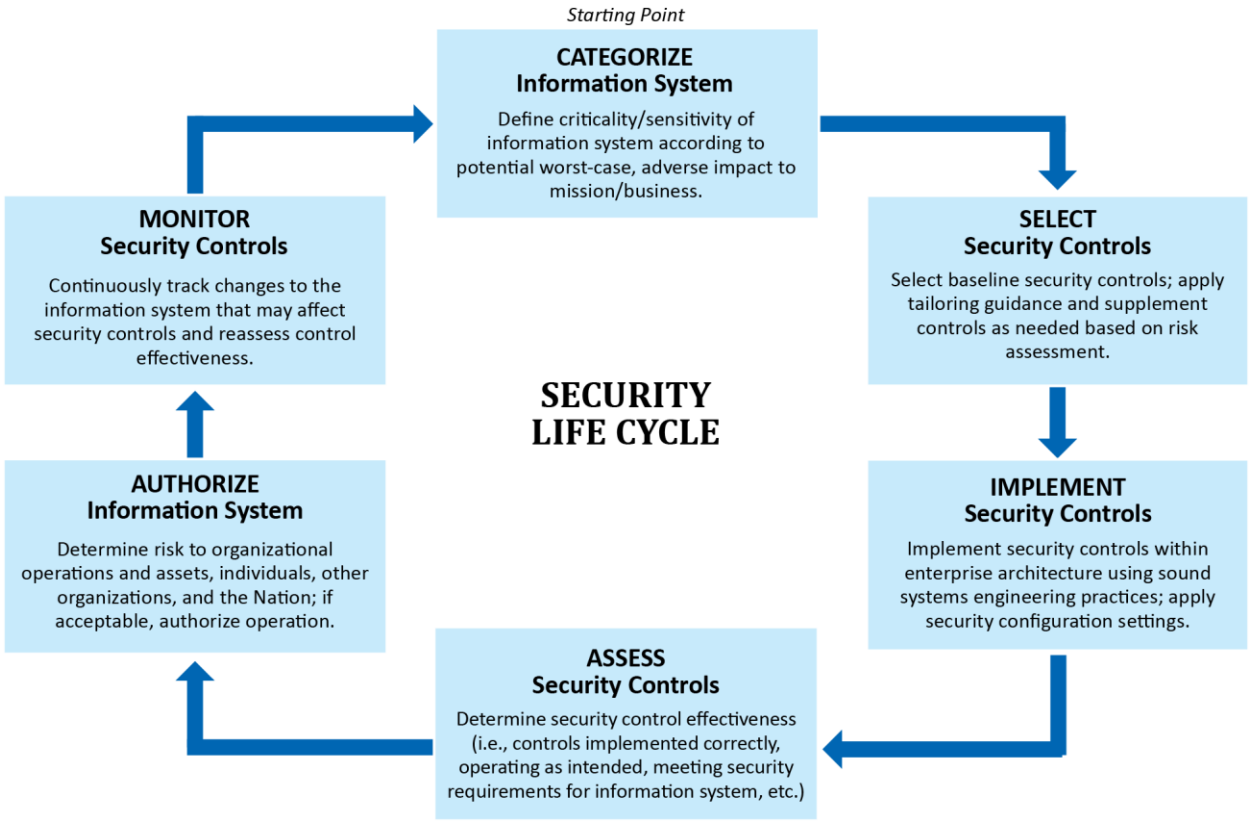
2. maintaining awareness of the security state of information systems on an ongoing basis through enhanced monitoring; and

3. providing essential information to senior leaders to facilitate decisions regarding the acceptance of risk to organizational operations and assets, individuals, and the Nation arising from the operation and use of information systems.

[3] This update of NIST SP 800-37, Revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach," February 2010, provides guidance on monitoring security controls in an operational environment.

Figure 2 illustrates the six step Risk Management Framework.

Figure 2: NIST Risk Management Framework



Source: NIST SP 800-37 Revision 1.

The guidelines provide basic concepts for managing information system-related security risks, including

- incorporating risk management principles and best practices into organization-wide strategic planning considerations, core missions and business processes, and supporting organizational information systems;
- integrating information security requirements into system development life cycle processes;
- establishing practical and meaningful boundaries for organizational information systems; and
- allocating security controls to organizational information systems as system-specific, hybrid, or common controls.

The guidelines emphasize that managing information system-related security risks is a complex, multifaceted undertaking that requires involvement by the entire organization – from senior leaders providing strategic vision and top-level goals and objectives, to mid-level leaders planning and managing projects, to individuals on the front lines developing and operating the systems that support the organization's core missions and business processes. The guidelines also highlight the importance of undertaking risk management early in the system development life cycle.

NIST Guide to Industrial Control Systems Security

A 2015 update of NIST standards on industrial control system security provides guidance on applying the NIST Framework and supplemental guidance to OT environments.[4] Specifically, major security objectives for an OT system implementation include

- restricting computer log-in access to the OT system network and network activity;
- restricting physical access to the OT system network and devices using controls such as locks, card readers, and security guards;
- protecting individual industrial control system components by timely deploying security patches after testing under field conditions, disabling all unused ports and services, restricting user privileges to only those required, monitoring audit trails, and using security controls such as antivirus software and file integrity checking software where technically feasible to prevent, deter, detect, and mitigate malware;
- maintaining functionality during adverse conditions; and
- restoring the system after an incident.

According to the guidance, it is essential for a cross functional cyber security team to include, at a minimum, IT staff, a control engineer, a control system operator, a network and system security expert, a member of the management staff, and a member of the physical security department to evaluate and mitigate risk to OT systems. For continuity and completeness, the cyber security team should also consult with the control system vendor or system integrator.

In addition, OT system implementation should use multi-layered security – commonly referred to as a "defense-in-depth strategy" – to minimize the impact of a failure in any one mechanism. This approach uses security countermeasures across operational, network, and device functionalities to protect the entire architecture. Effectively implementing this strategy requires contrasting the different challenges facing IT and OT systems. For example, in a typical IT system, data confidentiality, integrity, and availability are primary risk management concerns. While availability is also an issue for OT, human safety and fault tolerance are the primary concerns, and therefore personnel responsible for operating, securing, and maintaining OT must understand the link between safety and security. See Appendix B for the complete list of challenges identified by NIST.

DHS Industrial Control Systems Cyber Emergency Response Team

DHS's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) works to reduce security risks in critical infrastructure by partnering with law enforcement agencies; the intelligence community; Federal, state, local, tribal, and territorial governments; and control systems owners, operators, and vendors. ICS-CERT provides Federal agencies with a comprehensive review and evaluation of their industrial control system operations, focusing on network architecture, integration of IT and OT teams, vendor support, monitoring, cyber security controls, and internal and external connections.

[4] NIST SP 800-82.

Upon completion of its review, ICS-CERT compiles a report that offers discoveries and mitigation strategies for enhancing an organization's cyber security posture. During this audit, the NASA Office of Inspector General (OIG) observed the efforts of ICS-CERT in its review of select NASA control system environments.

DHS Continuous Diagnostics and Mitigation Program

The Continuous Diagnostics and Mitigation (CDM) Program is another effort by DHS to help Federal agencies secure their data and information systems. Through this initiative, DHS provides agencies with commercial off-the-shelf IT security tools to help system administrators identify cyber security risks in their networks, including current vulnerabilities and configuration settings. CDM is scheduled to be implemented across all Federal agencies, and in September 2015, DHS awarded a contract to Booz Allen Hamilton to implement CDM services at NASA and other agencies. At the time of our audit, NASA officials were working with Booz Allen to integrate the necessary information security tools for initial deployment.[5] Ultimately, CDM's success will depend on collaboration across functional boundaries within NASA to ensure all assets are appropriately accounted for and interdependencies identified and secured.

The Interagency Security Committee's Evaluation of Existing Cyber Security Standards and Facility Screening Criteria

In February 2015, the Interagency Security Committee released a white paper examining the efficacy of existing cyber security standards and facility screening criteria.[6] The Committee made several observations regarding the integration of IT/OT system security in the risk assessment framework for Federal facilities. First, they found existing standards do not adequately articulate cyber elements that should be considered and managed. Second, the standards must address interrelated hazards and cyber security threats to OT systems. Third, assessments of Federal cyber and physical critical infrastructure are done independently, and current assessment methodologies do not address the integration of cyber and physical characteristics. Based on these observations, the Committee made the following recommendations:

- Risk integration and vulnerability assessments should include cyber and physical security professionals in all phases of developing an appropriate risk assessment methodology, conducting risk and vulnerability assessments, and recommending appropriate countermeasures and/or protocols.
- Physical assessors must examine the systems already included in the physical security assessment to determine if they are dependent, operated, or connected through cyber or virtual means and to assess each component's existing security controls. Many of these systems are co-located with or linked to cyber-infrastructure components, and although physical security assessors have often evaluated integrated (cyber/physical) systems in the past, the focus was solely on the physical controls and access rather than the protection, integrity, and accessibility of cyber-enabled systems.

[5] NASA will be responsible for sustaining the effort once implementation is complete.

[6] Interagency Security Committee, "Presidential Policy Directive 21 Implementation: An Interagency Security Committee White Paper," February 2015. The Committee's mandate is to enhance the quality and effectiveness of the physical security and protection of buildings and nonmilitary Federal facilities in the United States and is made up of chief security officers and other senior executives from 60 Federal agencies and departments.

- Identification of threat category should include potential target attractiveness features and facilities should be categorized based on these features.

Finally, the Committee noted the importance of identifying utility penetration points for commercially provided systems like electric power, water, and natural gas, as well as the controls needed to access these systems.

NASA Policies Governing Agency Critical and Supporting Infrastructure

To implement national policy on critical infrastructure security and resilience, NASA has updated its regulations by defining which of the Agency's assets should be designated as NASA critical infrastructure and interdependencies (e.g., electric power and telecommunication systems), and devising a NASA Critical Infrastructure Protection Program (Protection Program) to secure these assets.[7]

NASA Critical Infrastructure

NASA regulations define critical infrastructure as "those essential facilities, missions, services, equipment, and interdependencies that enable the Agency to fulfill its national goals and Agency essential missions."[8] NASA's critical infrastructure may include IT resources; communication, command and control capabilities; Government-owned flight or experimental flight vehicles; the International Space Station; and other one-of-a-kind irreplaceable facilities.[9]

Interdependencies

Interdependencies include electrical power, gas, communication hubs, and local area networks. While interdependencies are not considered NASA critical infrastructure and need not be identified separately, they must be considered as part of each NASA Center's Protection Plan, evaluated for security risks, and protected. This is especially important for interdependencies that are "single points of failure," meaning their loss will compromise the operation of an asset.[10]

---

[7] Presidential Policy Directive (PPD) 21, "Critical Infrastructure Security and Resilience," February 2013, directs Government agencies to establish a program to identify their critical infrastructure or key resources, prioritize and evaluate their critical infrastructure or key resources for vulnerabilities, and fund appropriate security enhancements necessary to mitigate identified vulnerabilities. PPD-21 defines security as "reducing the risk to critical infrastructure by physical means or defensive cyber measures to intrusions, attacks, or the effects of natural or manmade disasters" and resilience as "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions . . . including the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents."

[8] NASA Procedural Requirements (NPR) 1600.1A, "NASA Security Program Procedural Requirements," August 12, 2013.

[9] Agency asset owners are directed to use the following definitions when considering whether to include an asset: (1) if its destruction or damage would cause significant impact on national economic security, national public health, safety, psychology, or any combination; (2) if a cyber security incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security; and (3) if its damage or destruction would have a debilitating impact on the ability of NASA to perform its essential functions and activities.

[10] NPR 1600.1A. NASA regulations do not address how Centers are to protect interdependencies operated by outside entities like electric and gas utilities.

Critical Infrastructure Protection Program

The Assistant Administrator for the Office of Protective Services (OPS), working with Center Critical Infrastructure Assurance Officers (Assurance Officers), oversees NASA's Agency-level Protection Program. NASA's Chief Information Officer, in coordination with Center Chief Information Officers, oversees protection of cyber-infrastructure assets and interdependencies and coordinates critical cyber-infrastructure identification, prioritization, and protection requirements with the Agency Critical Infrastructure Assurance Officer. All Center-level Protection Program activities are overseen by the Center Chief of Protective Services/Center Chief of Security (Security Chief) in coordination with Assurance Officers. Further, the Security Chief – using intelligence information (e.g., NASA's counterintelligence/counterterrorism program, local law enforcement, the NASA OIG, and other Federal agencies) – continuously evaluates Center- and program-level criticality, vulnerabilities, and local threats, and prepares countermeasures for inclusion in the Protection Program. Finally, the Assistant Administrator for OPS and the Security Chief, in conjunction with other NASA programs, directorates, or offices, are responsible for developing security guidance based on best practices.

Previously Identified Concerns Surrounding Information Technology Management at NASA

Over the last 6 years, the OIG has issued 21 audit reports containing more than 80 recommendations designed to improve NASA's IT security. In June 2013, we reported that NASA has struggled to implement an effective IT governance approach that appropriately aligns authority and responsibility commensurate with the Agency's overall mission.[11] In addition, during our fiscal year 2015 Federal Information Security Modernization Act review, we noted that even as NASA works to achieve more effective IT governance and risk management practices, IT security remains a significant challenge for the Agency.[12] In 2014, the Agency embarked on a comprehensive effort to address the technical capabilities required to support NASA goals from a strategic perspective. As part of a follow-on exercise, officials concluded the Agency lacks an enterprise-wide information security risk management framework. While NASA has since developed an Agency-wide Information Security Program Plan, finalization of the Plan is not expected until December 2019.

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

[12] NASA OIG, "Federal Information Security Management Act: Fiscal Year 2015 Evaluation" (IG-16-002, October 19, 2015).

NASA Lacks Comprehensive Security Planning for Managing Risks to Its Operational Technology Systems

NASA has not established clear guidance to define and secure its OT, is managing its OT systems without an adequate security plan, and is not following best practices for securing OT. Moreover, NASA's policies do not distinguish OT from IT, and the Agency does not offer training focused on protecting OT systems. As a result, NASA is not well-positioned to meet the security demands of an evolving OT environment and is assuming unnecessary risk for many critical Agency systems and facilities that incorporate OT components.

Defining Operational Technology

The operation of many of NASA's critical assets, including wind tunnels, rocket engine test stands, and thermal vacuum chambers, depends on actuators, valves, sensors, programmable logic controllers, and other OT components. In addition, OT components are critical to the operation of such underlying systems as water treatment, power, and chemical and gas storage. Despite its significant presence across the Agency and its criticality to the success of NASA's multi-faceted mission, the Agency has not adequately defined OT or established a standard protocol to protect systems that contain OT components. Moreover, it lacks a centralized inventory of OT systems.

Aircraft Test in NASA Wind Tunnel

Source: NASA.

The NASA Security Operations Center serves as the Agency's centralized resource to help ensure the security of data and information stored on NASA networks. However, unlike with NASA's institutional IT systems, Security Operations Center officials do not have visibility into the OT components deployed across the Agency and are therefore unable to identify and monitor OT-related threats or provide security controls specific to OT systems and facilities.

NASA maintains a cyber security database to track traditional enterprise IT systems, but only a fraction of OT assets are identified in the database. Specifically, of the 397 systems listed in the database, 32 reported having OT components. For the reasons discussed below, we believe the majority of OT systems at NASA are not reflected in this central repository.

First, the other 365 systems listed in the database include tracking and telemetry systems, wind tunnel control systems, and command and control systems, all of which contain significant OT components. Second, three NASA Centers did not list any OT systems in the database. However, when we visited two

of these Centers, we identified nearly 100 control systems.[13] Third, although we would expect all Centers to have utility control and monitoring systems, several Centers did not identify these systems as OT assets in the database. Similarly, only a single Center identified its fire alarm system in the database as an OT component. Finally, we identified an energy substation at one Center that supports an asset the Agency has deemed critical infrastructure that was not identified as an OT asset, lacked a security plan, and failed to account for connections to the NASA corporate IT network that could be used to infiltrate the energy substation control system or access NASA's IT network in search of other targets.

One of the reasons it is important to know which NASA systems incorporate OT components is because traditional IT security practices – when applied to OT systems – can cause the underlying systems to malfunction. For example:

- A large scale engineering oven that uses OT to monitor and regulate its temperature lost this ability when a connected computer was rebooted after application of a security patch update intended for standard IT systems. The reboot caused the control software to stop running, which resulted in the oven temperature rising and a fire that destroyed spacecraft hardware inside the oven. The reboot also impeded alarm activation, leaving the fire undetected for 3.5 hours before it was discovered by an employee.

Electric Walk-in Oven, Post Fire

Source: NASA.

- Vulnerability scanning used to identify software flaws that can be exploited by an attacker caused equipment to fail and loss of communication with an Earth science spacecraft during an orbital pass. As a result, the pass was rendered unusable and data could not be collected until the next orbital pass.
- Disabling of a chilled water Heating, Ventilation, and Air Conditioning (HVAC) system supporting a data center caused temperatures to rise 50 degrees in a matter of minutes, forcing shutdown to prevent damage to critical IT equipment.

Generally, we found the security protocols NASA applies to OT systems are intended for traditional IT systems. However, due to unique performance, reliability, and safety requirements, OT systems often require adaptations and extensions to security standards. NIST guidance describes how to develop specialized sets of controls, or overlays, tailored for specific types of missions or business functions, technologies, or environments, but NASA has not implemented this guidance.

Security Plan Development

NASA policy requires all information system owners to maintain security plans based on NIST guidance. However, the Agency did not require system owners to create security plans tailored to OT systems.

[13] We did not visit the third Center.

Categorizing Operational Technology within NASA's Environment

We found that NASA was not following NIST guidance and failed to properly categorize its OT systems. As noted earlier (and displayed in Figure 2), the first step in the NIST Risk Management Framework is to categorize systems to ensure proper security controls are adopted. During categorization, system owners describe the purpose of the system in detail and identify hardware, software, unique protocols, and any associated OT.[14]

The Framework and related NIST criteria identify critical security control overlays, best practices, and other actions to protect OT systems from cyber and physical manipulation. However, we did not identify any NASA security plans that incorporated or even cited NIST guidance for control systems. Failure to appropriately categorize Agency systems can lead to inadequate security or the application of controls that can damage OT systems, leading to cascading security gaps throughout the risk management process. Such gaps place physical assets and sensitive data at risk of loss or disclosure.

Because many of NASA's systems contain both IT and OT components, both aspects must be considered when developing security plans. As we discuss in more detail below, Agency Office of the Chief Information Officer (OCIO) and OPS officials do not coordinate their security assessments. Moreover, although they are largely responsible for the environmental control infrastructure surrounding NASA's cyber and physical assets, the Office of Strategic Infrastructure (OSI) is not part of either Office's assessment. The lack of coordination between these parties in developing security assessments creates gaps and inefficiencies that have resulted in disruptions to NASA operations and damage to NASA assets, such as the oven fire described above.

As one step in categorizing system risk, NIST recommends defining information system boundaries by the type of information the system manages. We found NASA is not accurately defining these boundaries because individual systems are being grouped into a single security plan. At one Center, we discovered more than 90 OT control systems grouped into one "moderate impact" security plan that included critical infrastructure systems. We identified similar groupings at other Centers, although not of this magnitude.

Failing to make the distinction between traditional IT and control OT systems and grouping systems with varying risk impact levels into a single security plan during system categorization calls into question the accuracy of NASA's risk categorization and impacts the level of protection and resources allocated to individual systems. For example, a system inaccurately categorized as "high risk" may be allocated unnecessary security resources while one inaccurately categorized as "low risk" may not be adequately protected.

We found multiple OT or hybrid IT/OT systems were often grouped into single security plans because of the high cost of conducting individualized security assessments and maintaining separate security plans. At one Center, costs for such assessments – which are required for each security plan established – started with a $12,000 base charge and increased by $210 per system component, capping out at a maximum charge of $60,000 per year, per system plan. Further, the assessments were based strictly on a traditional IT system and did not take into consideration that a subset of the systems were OT critical infrastructure components.

[14] NIST recommends that for systems with OT, NIST SP 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," Appendix F, April 2013, and NIST SP 800-82 be used as guidance for applying proper security controls.

According to Agency personnel, high security assessment costs may be reduced or eliminated as a result of a proposed initiative to use internal independent assessors in lieu of external sources, a plan developed by NASA's IT management Business Services Assessment. While this may address the cost concerns associated with assessing system security plans, identifying the appropriate categorization of the system and its components and the resulting accuracy of these security assessments remains a concern.

Awareness and Training

DHS and NIST offer comprehensive guidance and best practices for securing OT while DHS's ICS-CERT offers no-cost training on OT security. Other organizations, such as the cyber security certification body of the SANS Institute, have adopted the NIST standards and also offer control system security training. Although the OT security field has evolved and matured over the past few years, NASA has not adopted this discipline into its security planning process.

HVAC Smart Damper/Actuator

Source: Schneider Electric.

We visited five Centers and NASA Headquarters as part of this audit and interviewed Agency officials from OCIO, OPS, and OSI, as well as multiple system owners and system administrator personnel to gauge their level of control system security awareness and training. Of the more than two dozen people we interviewed, only one had received any control system security training. Similarly, although NASA and NIST require role-based IT training as part of their IT security requirements and additional training for individuals with significant security responsibilities, including users with privileged network user accounts and those with managerial, administrative, or operational responsibilities, NASA does not require role-based OT-specific training.[15]

Security awareness plays a critical role in preventing potentially damaging cyber security incidents. For example, a programmable controller for a data center's HVAC system housed in a basement or closet may appear low risk and therefore not a candidate for inclusion in a security plan. However, an adversary with physical or logical access could compromise the controller and shut down the system, leaving the data center's computers without the cooled air required to operate. A coordinated risk assessment by trained personnel across functional boundaries would better position NASA to identify such risks and take appropriate actions to mitigate them.

ICS-CERT provides frequent alerts and advisories for OT system owners and operators, including actual events and vulnerabilities that have taken place in control system products. We found NASA is not using these alerts and advisories to help manage its OT security.

[15] Role-based training is required as per NASA IT Security and Training Handbook 2810.06-02, "Awareness and Training: Role-Based Training," February 2016; NIST SP 800-16, "Information Technology Security Requirements: A Role- and Performance-Based Model," April 1998; and NIST SP 800-53.

Challenges Implementing Security Controls in NASA's Operational Technology Environments

Historically, OT systems bore little resemblance to traditional IT systems in that they were isolated and operated proprietary protocols using specialized hardware and software. As these systems evolve and become more interconnected with IT networks, the possibility of cyber security vulnerabilities and incidents increases.

Under the Federal Information Security Modernization Act, NASA is required to implement controls that eliminate or reduce risk to an acceptable level while maintaining the operational state of its systems. One of the biggest challenges NASA faces in applying traditional IT security practices to an OT environment is that OT architectures are often aging, isolated, and lack strong processing capability. Logically and physically isolated systems do not conform well to NASA's automated application of common security controls, which in many cases requires that software and network connectivity be available in the OT environment. Further, while aging NASA legacy OT systems, such as wind tunnels and rocket propulsion control systems, are being retrofitted to utilize modern IT components, this evolution is not consistently captured in the security planning process, leaving security personnel unaware of the changes and the need to add security controls to mitigate risks.

Further complicating the application of security controls is that NASA's OT often operates in an environment that includes both robust IT and sensitive OT components with less processing power. As the oven fire example discussed above illustrates, application of routine security controls designed for traditional IT systems on an OT system can result in disruption of system operations and endanger assets and human life. Accordingly, it is critical to ensure inventories capture sufficient detail to identify the ability of assets to support application of security controls.

As noted above, NASA has not yet adopted policies and practices recommended by ICS-CERT and NIST guidance related to OT. In our judgment, this omission, coupled with insufficient collaboration and an overall lack of awareness of OT security at the Agency, raises serious concerns. While implementation of the CDM security tool suite may not address security concerns in all of NASA's OT environments, proper identification of the Agency's OT systems along with the implementation of a network segmentation strategy – results anticipated from the CDM initiative – should bring much needed cyber security resources to projects that have otherwise been left without comprehensive cyber security management.

Lack of Internal Monitoring, Auditing, and Log Management Capabilities

To protect OT systems at the Centers we visited, NASA relied primarily on the systems' perceived physical or logical isolation from larger Agency networks. However, as NASA's OT systems become more sophisticated and connected to traditional IT networks, this isolation is likely to prove inadequate. For example, we identified OT systems NASA officials believed were physically isolated but were actually connected to larger Agency networks. If not properly secured, such connections could provide unauthorized access through less trusted, internal Agency networks. Further, responsible personnel were not performing sufficient traffic monitoring, internal auditing, or intrusion detection on the OT systems and therefore lacked comprehensive awareness of their security posture. As part of its review, DHS examined three OT systems at two Centers and determined they lacked sufficient

monitoring of internal traffic, auditing capabilities, and log management. In addition, using a similar methodology as DHS, we identified a lack of continuous monitoring at three other NASA locations that housed multiple OT environments.

Use of Group Accounts

With a single exception, we found all of the control system environments we assessed were utilizing group accounts (i.e., a single login credential used by multiple individuals) to manage OT systems. These included systems that control Center utilities, such as water and power, and mission systems, such as telemetry and tracking and wind tunnel control systems. The use of group accounts does not provide for individual accountability because there is no way to tell which user is actually accessing the system. In addition, having shared accounts increases the likelihood that unauthorized individuals may gain access to the password due to increased risk of inadvertent disclosure. Despite these risks, we found enhanced physical security measures were not consistently implemented in accordance with Federal guidance and security best practices for these systems. Unauthorized changes to these systems could damage or disable equipment, create environmental impacts, or endanger human life. In a typical computer program, a single variable could simply be a "yes" or "no" instruction. In an OT system, however, a single variable could result in an "open" or "close" command for a valve controlling a volatile liquid or gas and an unauthorized change to such a simple script could lead to a catastrophic environmental impact. NIST illustrates this scenario by citing the example of a sewage spill in Australia where a disgruntled employee altered electronic commands for sewage pumping stations causing them to malfunction, resulting in the release of 264,000 gallons of raw sewage into nearby rivers and parks.

According to NASA officials, individual account management controls had not been implemented on some of these systems because they need to run continuously to meet mission needs and therefore cannot tolerate the downtime associated with logging off or setting time limitations on individual user sessions. On other occasions, controls were missing because the Agency has not required their use. Further, we noted the absence of compensating controls such as closed-circuit television, intrusion detection systems, and enterprise physical access control systems. We also found that rather than using compensating measures as directed in NIST guidance for securing control systems, risks were often simply accepted in the security plans without adoption of compensating measures.

Configuration Management and Settings

A configuration baseline is a description of the security attributes of a system at a point in time that serves as a basis for documenting subsequent changes. The OT environments we assessed lacked approved security configuration baselines, and deviations from the required security settings had not been properly documented in system security plans.[16]

As with traditional IT systems, local system security administrators should configure OT systems, services, and applications to maintain the minimal level of required functionality to reduce security risks.[17] For example, an administrator should disable all unneeded ports, services, and applications on

[16] NASA-STD-2804, "Minimum Interoperability Software Suite," May 2016, provides guidelines for software security configuration settings. Baseline is a term used for security configurations which have been approved and mandated for use Agency-wide. Any deviations from approved baseline security settings should be documented and authorized during security planning.

[17] NIST SP 800-53, Revision 4, Control CM-7 Least Functionality.

components connected to an OT system to reduce the possibility that malicious actors can penetrate the network through unused functions – essentially, closing "doors" that do not need to remain open. This control needs to be scrutinized in greater detail in OT system environments because of the operational state of the system components.

For example, HVAC control systems that utilize "smart" thermostats with wireless capabilities enable remote management and communication between other smart devices, computers attached to the local area network, or even with the product developer through the Internet. Accordingly, a poorly configured HVAC system thermostat with an unneeded network connection could provide an avenue for a cyber attack. Even if disabling remote connection capabilities is not an option, proper network segmentation and other controls can act as compensating security measures. At NASA, these types of devices are the responsibility of OSI personnel who are generally not involved in cyber or physical risk management for Agency control systems and lack the security expertise to implement compensating security measures.

When applying security controls, OT operators must thoroughly test all of the settings within a security configuration baseline for a particular piece of software. In some cases, this may entail testing hundreds of settings to ensure they do not impact operation of the system while providing the desired level of protection. This makes it particularly important that security is considered early in the planning stages of an OT system. For example, failure to test security baselines can result in inadvertently disabling a programmable logic controller for fire suppression, deactivating important alerts, or an unplanned automated lock up of the system. Moreover, a complete lack of security configuration baselines can result in the compromise of OT systems by malicious actors, inefficient configurations that unnecessarily consume system resources, or open ports that enable malicious scanning of the system.

Media Protection

We identified a lack of controls for removable media in the locations we visited, including the use of USB storage devices and outside vendor laptops used to perform maintenance on OT systems. Removable media can introduce malware into an OT system even when locations are physically or logically isolated from larger Agency networks. The danger from removable media can be controlled with proper settings or configurations applied directly to the OT system or through compensating manual measures.

Given that NASA does not differentiate between IT and OT when performing risk assessments on OT systems, security controls particularly relevant to OT systems can be overlooked. Moreover, controls such as malware detection software readily available in a traditional IT environment are not as common in OT environments. For example, in isolated OT environments such as an electrical substation, malware detection capabilities may not be available. As a result, a best practice would be to disable removable media capabilities, including USB drives or optical disks. If malware detection mechanisms exist, then additional controls, such as disabling the function that allows removable media to run automatically (e.g., when a CD automatically initiates upon entry into the drive) should be applied. Further, ensuring OT vendor support equipment is thoroughly inspected prior to allowing such equipment to connect to OT system environments is important. However, we found this was not consistently happening in the environments we assessed because malware detection capabilities were largely unavailable to scan vendor equipment in advance of connectivity.

Network Segmentation

We found multiple instances of OT networks lacking internal network segmentation, which could lead to access from less-trusted networks. As IT and OT networks become more interconnected, the need to segment networks from corporate IT using a solution such as a demilitarized zone network configuration becomes more important.[18] The lack of segmentation in OT system environments is at the top of the ICS-CERT team's findings across all systems they assess. Attackers use networks with limited separation to establish a foothold in an OT system network, exploit that system, and move into the entity's larger IT network. In addition, malware protections, monitoring agents, and software patching on the physically isolated networks we identified cannot be deployed without some form of segmentation strategy. Further, applying a well-documented network segmentation strategy could improve NASA's planned CDM implementation by allowing physically and logically isolated assets access to the CDM tool suite. We identified one Center working toward segmenting all control/OT systems from their institutional networks. However, planning for this effort was in the early stages and the team had no dedicated funding for implementation.

[18] A demilitarized zone is a physical or logical subnetwork that contains an organization's external-facing services to a larger and untrusted network such as the Internet. The purpose of a demilitarized zone is to add an additional layer of security to an organization's local area network.

NASA's Critical Infrastructure Assessment and Protection Could Benefit from Improved Operational Technology Security

NASA lacks an integrated approach to managing risk associated with its critical infrastructure that incorporates physical and cyber security considerations in all phases of risk assessment and remediation. For example, the security of physical and cyber components of NASA's critical assets is managed with minimal collaboration among key Agency stakeholders and does not involve the OSI even though the Office manages the supporting infrastructure associated with critical assets. This disjointed approach has led to duplication of effort and gaps in security planning and risk remediation at both the Agency and Center levels. Further, based on the inconsistent security practices we observed at the various Centers, we question the overall efficacy of NASA's critical infrastructure identification process. Finally, inadequate guidance and oversight, coupled with insufficient record keeping and funding, limit the visibility and insight responsible personnel have into NASA's critical infrastructure protection processes and impairs their ability to protect Agency assets.

Lack of an Integrated and Collaborative Approach

NASA personnel who manage the assessment and protection of NASA's critical infrastructure carry out their responsibilities independent of one another, which has resulted in a failure to adequately address interrelated hazards to hybrid IT/OT systems. Federal guidance emphasizes the importance of approaching the security and resilience of critical assets in an integrated, holistic manner. At NASA, issues of risk management and security controls span functional boundaries, requiring the involvement of personnel from NASA Mission Directorates, OCIO, OPS, and OSI. While the Assistant Administrator for OPS and the Agency Chief Information Officer are charged with coordinating and overseeing NASA's Protection Program, the Program needs to provide key participants with comprehensive support and oversight. An Agency-level OPS official informed us they rely on Center-level OPS staff to identify and assess risk and to protect Agency critical and supporting infrastructure at the Centers. However, Center OPS staff said they struggle with implementation of critical infrastructure security requirements and need additional guidance from Agency OPS.

Further, in spite of increased interconnectivity among physical and cyber assets at NASA, Agency-level OPS and OCIO assessments of Agency physical and cyber critical infrastructure are undertaken independently and current risk assessment practices do not address the integration of physical and cyber characteristics of the infrastructure. Moreover, neither Office has insight into the other's assessment methodology and, except when OCIO identifies a cyber asset as critical and submits that determination to OPS for consideration, they do not coordinate their efforts.

This disjointed approach at the Agency level has a cascading effect on the way Center OPS and OCIO personnel handle critical infrastructure security. Similar to Agency-level assessments, Center OPS and OCIO carry out risk assessments of physical and cyber assets independently. This lack of collaboration at both Agency and Center levels is notable because while OPS personnel are responsible for the physical security of NASA critical infrastructure, OCIO personnel are uniquely qualified to identify and assess cyber-specific risks to those assets and implement appropriate safeguards.

Insufficient Guidance and Oversight

We identified inconsistencies in the assessment method and criteria Centers use to designate assets as critical infrastructure. For example, one Center we visited had removed all its assets from NASA's critical infrastructure inventory after retirement of the Space Shuttle. Conversely, another Center listed 12 assets on the inventory in an effort to help secure resources to protect the assets. In our assessment, these differing approaches are equally undesirable as one creates gaps in the security of critical assets while the other may lead to unnecessary spending to protect noncritical assets. Ultimately, NASA's critical infrastructure inventory may not be meeting its purpose of ensuring Agency-wide uniformity and consistency in performing appropriate security risk assessments.

Center OCIO and OPS officials we interviewed attributed the inconsistencies in part to inadequate Agency-level guidance and oversight of Center activities. These officials informed us they have difficulties interpreting and implementing NASA critical infrastructure security regulations and controls. For instance, Center OCIO and OPS personnel said they found the Agency's critical infrastructure definition and criteria vague and overly inclusive, which made it particularly difficult for Centers to dedicate scarce resources to security measures. For example, a Center OPS Chief told us that a building with more than 160 doors designated as critical infrastructure at his Center would cost an estimated $800,000 to $1 million to bring into compliance with Agency security requirements. Follow-on assessments that incorporated the underlying IT requirements needed to support physical security implementations revealed that this estimate was significantly understated and that the necessary infrastructure modifications and security protections could cost as much as $6.9 million. Providing enhanced security to Center facilities like this results in a considerable financial burden to Centers.

Center OPS staff also need guidance on how to prioritize NASA's critical infrastructure assets. According to NASA regulations, "the Center/Facility Security Level (FSL) allows Center management to prioritize assets so that physical security resources can be applied in the most efficient and cost-effective manner possible, and to establish asset protection programs appropriate for their value and the likelihood of an attempt to compromise them."[19] However, these regulations do not specify how Centers should prioritize security planning among assets of national criticality and those with only NASA-wide or Center-specific importance.

Further, Center officials find the risk assessment form used for critical infrastructure record keeping inadequate because it does not capture the criticality level and security needs of the interdependencies that support NASA's critical infrastructure. Without this information, OPS and other security personnel who assess infrastructure assets are unable to determine whether and to what extent the assets are dependent on, operated, or connected through cyber or virtual means. This deficiency hinders their ability to effectively assess and remediate security risks.

[19] NPR 1620.3A, "Physical Security Requirements for NASA Facilities and Property," October 2012.

We also found that Center facilities, maintenance, and operations management personnel have generally been excluded from physical and cyber security risk management processes even though they oversee vital interdependencies such as HVAC, power distribution, water, gas, and fire suppression. We found their involvement in protecting NASA critical infrastructure was limited to rare occasions of informal consultation with Center OPS staff during initial stages of facility designations. At one Center, we identified facilities and OT systems directly responsible for backup power generation that had no security plan. At another Center, we identified HVAC control systems that provided vital cooling services to a NASA critical infrastructure data center that had not been sufficiently considered during security planning. Moreover, NASA regulations do not include OSI or Center-level facilities and operations management as part of the Protection Program.

Finally, we found Centers were unclear about how to implement interdependency requirements and consequently rarely treat supporting infrastructure any differently than non-critical infrastructure. Center OCIO and OPS officials cited a need for supplemental guidance on identifying, documenting, and protecting interdependencies. For example, when evaluating assets for NASA critical infrastructure designation, asset owners are directed to consider critical infrastructure interdependencies (e.g., IT resources, data, electric power, water, oil and gas, and environmental control networks) that support NASA's critical assets and whose loss could directly impact NASA's essential mission capability. However, neither the forms used to designate the assets criticality nor the facility security assessments themselves include elements to support consideration of such interdependencies. We also found Center OPS officials are unclear what additional security controls should be applied for interdependencies that are single points of failure – such as electrical and water supply systems owned or operated by entities other than NASA. All Center OPS officials we interviewed indicated they do not differentiate between interdependencies that are single points of failure and those that are not and need guidance from the Agency on how to evaluate potential vulnerabilities.

CONCLUSION

NASA utilizes a wide array of IT and OT to test rocket propulsion systems, control and communicate with spacecraft, and operate ground support facilities. Indeed, 65 percent of NASA's critical infrastructure assets are operated using OT or hybrid IT/OT systems. As this infrastructure becomes more interconnected and complex, NASA faces an increased risk of cyber threats that could compromise missions and underlying Agency IT systems and networks.

Although NASA has developed policies for securing IT and physical assets, it has not yet identified and defined its OT footprint or adopted best practices to secure its OT systems. Moreover, disjointed silos of expertise have led to control deficiencies and a lack of engagement among OT operators, system owners, and IT security personnel. Similarly, a failure to adopt guidance has resulted in inefficiencies and significant gaps in security planning and OT risk remediation.

Further, NASA's management of critical infrastructure and related interdependencies face similar challenges and could be improved through increased awareness and collaboration across functional boundaries. Increased collaboration among NASA Mission Directorates, OCIO, OPS, and OSI prior to implementation of the upcoming CDM initiative is crucial to accurately identifying critical assets and improving the security of NASA's OT environment.

RECOMMENDATIONS, MANAGEMENT'S RESPONSE, AND OUR EVALUATION

To ensure NASA is adequately assessing risk for and applying security controls to its critical assets, we recommended:

1. The NASA Administrator, in conjunction with the Associate Administrator for Mission Support and NASA Mission Directorates, develop a framework to coordinate security efforts across the Agency that promotes uniformity of processes and procedures and enables collaboration between OCIO, OPS, and OSI.
2. The Assistant Administrator for OPS, in conjunction with the Agency Chief Information Officer, develop a standardized process to assess Agency cyber and physical assets for NASA critical infrastructure designation that adequately evaluates criticality to NASA's overall mission.
3. The Assistant Administrator for OPS ensure OCIO and OSI representatives are included in functional reviews of NASA's critical infrastructure assets and facility security assessments so that cyber and facility interdependencies are addressed appropriately.
4. The Assistant Administrators of OPS and OSI, in conjunction with the Agency Chief Information Officer, coordinate the development of a methodology for the identification and protection of interdependencies (either within the facility security assessment or facility security level designation process).
5. The Agency Chief Information Officer, in conjunction with the Assistant Administrators of OPS and OSI, develop security policy based on NIST Special Publication (SP) 800-53, Revision 4, and NIST SP 800-82 guidance for managing the protection of OT within the mission and institutional directorates. At a minimum, this should include
    a. defining control systems;
    b. identifying all OT systems at NASA and a strategy for segmenting OT from IT across the Agency;
    c. utilizing ICS-CERT alerts when assessing control systems security posture;
    d. developing system security plans and assessment methodologies for control systems/OT in a way that ensures the use of appropriate system boundaries and effective compensating controls, in the absence of common controls or automation as defined in NIST SP 800-82; and
    e. developing training for responsible security personnel in line with NIST and DHS guidance on control system security. This may include control system administrators, OCIO approval authorities, control system owners, and assessment teams.

To ensure NASA is adequately identifying critical infrastructure and supporting interdependencies and appropriately protecting its OT systems, we recommended NASA's Associate Administrator:

6. establish an integrated cyber and physical risk management committee or oversight body composed of subject matter experts from NASA Mission Directorates, OCIO, OPS, and OSI.

We provided a draft of this report to NASA management who concurred or partially concurred with our recommendations and described corrective actions the Agency has taken or will take to address them. For recommendations 2 through 5, the Agency partially concurred, pointing to the recent development and implementation of the Enterprise Protection Program (EPP), which the Agency says will focus on protecting strategically critical capabilities and technologies. However, the response describes the EPP and associated board as advisory in nature. Given the governance concerns we have highlighted in this and other reports, we encourage NASA to ensure EPP leadership has sufficient technical authority and support from other responsible components to direct the change required to meet the intent of our recommendations. We believe given the proper authority EPP can implement appropriate corrective action. Accordingly, our recommendations are resolved and will be closed upon completion and verification of the proposed corrective actions.

Management's full response to our report is reproduced in Appendix C, and technical comments have been incorporated as appropriate.

Major contributors to this report include Laura Nicolosi, Mission Support Director; Scott Riggenbach, Project Manager; Earl Baker; Jonathan Flugel; Sashka Mannion; Benjamin Patterson; and Chris Reeves.

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

Paul K. Martin
Inspector General

APPENDIX A: SCOPE AND METHODOLOGY

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

We initiated our review of industrial control systems within NASA's critical and supporting infrastructure to evaluate whether NASA is (1) identifying critical and supporting infrastructure and (2) protecting this infrastructure once identified. Specifically, we assessed systems and engaged responsible parties to determine if NASA has implemented effective physical and logical security controls necessary to protect these assets against cyber and physical security threats.

Through the course of this review we utilized NASA's critical infrastructure listing, systems inventory, IT security database, procedural requirements, documented industry best practices, and testimony by NASA and partner agency subject matter experts. We focused our efforts on key areas of risk management, security awareness, and continuous monitoring of OT systems. To determine if NASA was adequately identifying critical and supporting interdependencies, we reviewed current and past NASA critical infrastructure listings and NASA IT security system inventories in an effort to locate OT systems that supported critical infrastructure. Further, we queried the IT security database to identify OT systems that had not been identified as such. After identifying a subset of assets and systems, we performed in-depth assessments in line with the methodology used by ICS-CERT. We evaluated processes and systems at five NASA Centers against established best practices for the identification and protection of critical OT systems. Further, we held multiple interviews with responsible parties within the OCIO, OPS, OSI, and individual mission and institutional systems offices.

We evaluated NASA's directives, policies, and processes against established best practices identified in NIST and DHS guidance. Additionally, we reviewed presidential directives, Office of Management and Budget guidance, and Department of Defense guidance concerning critical infrastructure identification and protection and the security of operational technologies. Relevant guidance included:

- Homeland Security Presidential Directive 7
- PPD-21
- Federal Information Processing Standards publications
- Department of Defense Committee on National Security Systems Instruction 1253
- NIST SP 800-series
- Federal Continuity Directive 2
- NASA Procedural Directives, NPRs, and NASA IT Security Handbooks
- DHS Interagency Security Committee Standards "The Risk Management Process for Federal Facilities"

Use of Computer-Processed Data

We used computer-processed data to the extent of querying NASA's IT security database in an effort to identify system security plans marked as control systems. We validated the results against individual searches of the security plans identified.

Review of Internal Controls

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

Prior Coverage

During the last 6 years, the NASA OIG and the Government Accountability Office have issued eight reports of significant relevance to the subject of this report. Unrestricted reports can be accessed at http://oig.nasa.gov/audits/reports/FY17 and http://www.gao.gov, respectively.

NASA Office of Inspector General

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)

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

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

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

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

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

Government Accountability Office

Federal Facility Cybersecurity-DHS and GSA Should Address Cyber Risk to Building and Access Control Systems (GAO-15-6, December 12, 2014)

APPENDIX B: NIST IDENTIFIED CHALLENGES ACROSS INFORMATION TECHNOLOGY AND OPERATIONAL TECHNOLOGY SYSTEMS

The 2015 comprehensive update of NIST SP 800-82, "Guide to Industrial Control Systems Security," offered tailored guidance on how to adapt and apply the security controls and control enhancements detailed in NIST SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," to industrial control systems. It is important to contrast the challenges across IT and OT security risk management and control implementation. As highlighted in NIST guidance, these challenges include the following:

- *Timeliness and performance requirements.* OT systems are generally more time-critical than IT systems and require reliable deterministic responses. High throughput is typically not essential to OT, but automated real-time response to human interaction is often critical.
- *Availability requirements.* Many OT processes are continuous in nature, and unexpected outages are unacceptable. Outages must often be planned and scheduled well in advance and depend heavily upon exhaustive testing. Typical IT strategies, such as rebooting a component, are usually not acceptable due to adverse impact on the requirements for high availability, reliability, and maintainability of the control system.
- *Risk management requirements.* In a typical IT system, data confidentiality and integrity are primary concerns. For OT, human safety and fault tolerance are the primary concerns. Personnel responsible for operating, securing, and maintaining OT must understand the important link between safety and security.
- *Physical effects.* OT can have very complex interactions with physical processes. Understanding the potential physical consequences of an adverse event often requires communication among experts in different areas.
- *System operation.* OT operating systems and control networks often require different skill sets and levels of expertise from those of traditional IT. Failure to understand those differences can have disastrous consequences on system operations, such as failures of components supporting time critical operations.
- *Resource constraints.* OT often consists of resource-constrained systems that do not include contemporary IT security capabilities. Many are based upon legacy systems lacking resources and features that are common on modern IT systems (e.g., encryption capabilities, error logging, and password protection). Because there may be fewer computing resources available on OT components, retrofitting systems with security capabilities may not be possible.
- *Communications.* Communication protocols and media used by OT environments for field device control and intra-processor communication are typically different from most IT environments, and may be proprietary.

- *Change management.* Implementation of change management will vary significantly between IT and OT systems. For example, while software patches on IT systems are typically applied in a short timeframe, perhaps using automated means, software updates on OT systems require planning and testing and may not occur as quickly as IT updates. In addition, many OT systems utilize older versions of operating systems that are no longer supported by the vendor, and patches may not be available. The change management process, when applied to OT, requires careful assessment by OT experts (e.g., control engineers) working in conjunction with other personnel (e.g., security, IT, and operations staff).
- *Component lifetime and location.* For OT, the lifetime of the deployed technology is often on the order of 10 to 15 years (and sometimes longer), in contrast with 3 to 5 years for IT components. OT components may be distributed in isolated and/or remote areas and may not be easily reachable.

APPENDIX C: MANAGEMENT'S COMMENTS

National Aeronautics and Space Administration
Office of the Administrator
Washington, DC 201546-0001

January 31, 2017

TO: Assistant Inspector General for Audits

FROM: Principal Advisor, Enterprise Protection Program

SUBJECT: Agency Response to OIG Draft Report "Audit of Industrial Control System Security within NASA's Critical and Supporting Infrastructure" (A-16-001-00)

NASA appreciates the opportunity to review and comment on the Office of Inspector General (OIG) draft report entitled "Audit of Industrial Control System Security within NASA's Critical and Supporting Infrastructure" (A-16-001-00), dated December 21, 2016.

In the draft report, the OIG makes six recommendations intended to ensure NASA is adequately: 1) assessing risk for an applying security controls to its critical assets, and; 2) identifying critical infrastructure and supporting interdependencies and appropriately protecting Operational Technology (OT) management systems. Because the terminology is still in development, all discussion below noted as OT includes Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems.

While NASA concurs with the intent of each of the OIG's recommendations, we partially concur with recommendations 2 through 5 in order to reflect NASA's development and implementation of its Enterprise Protection Program (EPP) and its leadership role in response to each of these recommendations. In August of 2016, NASA established the position of Principal Advisor for Enterprise Protection (PAEP) within the Office of the Administrator and on 30 November the Agency Program Management Council (APMC) voted to make the EPP official. The PEAP was identified to lead the cross-Agency EPP and the Enterprise Protection Board (EPB). The EPB, an advisory entity which includes Associate Administrators from each mission directorate as well as the Chiefs from the mission support offices, will integrate all recommendations/issues from exiting or new Agency cyber, space, institutional, national security, and mission protection working groups through the PAEP. NASA recognizes that the development and implementation of the aforementioned program and board were early in their development phase during this audit.

The EPP has been established to address protection challenges through vulnerability, susceptibility, and mitigations and protections of all NASA missions and activities. The objective is to identify and implement protection recommendations into existing requirements, budgeting, acquisition, and design processes. This activity will focus on protecting strategically critical capabilities and technologies. NASA's overall objective is to create and install an Enterprise-level management system consisting of policy, procedures,

and requirements with checks and balances to protect and maintain NASA's strategically critical capabilities and technologies. Recommendation actions will be led by the PAEP, in coordination with the EPB, and final implementation plans will be presented to the APMC for decision.

Specifically the OIG recommends the following:

To ensure NASA is adequately assessing risk for and applying security controls to its critical assets, the OIG recommends:

Recommendation 1: The NASA Administrator, in conjunction with the Associate Administrator for Mission Support and NASA Mission Directorates, develop a framework to coordinate security efforts across the Agency that promotes uniformity of processes and procedures and enables collaboration between the Office of the Chief Information Officer (OCIO), Office of Protective Services (OPS), and Office of Strategic Infrastructure (OSI).

Management's Response: NASA concurs with this recommendation. The Agency Principal Advisor for Enterprise Protection is developing a framework to coordinate security efforts across the Agency that promote enterprise-level solutions and overall uniformity of processes and procedures which will enable collaboration between the missions and mission support offices such as the OCIO, OPS, and OSI. These offices, through the Industrial Controls Systems Working Group (ICSWG) identified in Recommendation 2, link directly to the EPB which will ensure threats are addressed across the Agency at an enterprise level.

Estimated Completion Date: October 1, 2018

Recommendation 2: The Assistant Administrator for OPS, in conjunction with the Agency Chief Information Officer, develop a standardized process to assess Agency cyber and physical assets for NASA critical infrastructure designation that adequately evaluates criticality to NASA's overall mission.

Management's Response: NASA partially concurs with this recommendation. NASA concurs with the intent of this recommendation, but not with the recommended implementation. The Principal Advisor for Enterprise Protection, charged with cross-Agency coordination of the EPP, will establish an ICSWG, to include OPS, OSI, and OCIO. The ICSWG will develop and enhance standardized processes to assess NASA's strategically critical capabilities and technologies designation, which would include cyber as well as physical assets that adequately evaluate criticality to NASA's overall mission. The ICSWG will report, as appropriate, to the EPB. The EPB will meet to address issues and inform the APMC.

Estimated Completion Date: October 1, 2018

Recommendation 3: The Assistant Administrator for OPS ensure OCIO and OSI representatives are included in functional reviews of NASA's critical infrastructure assets and facility security assessments so that cyber and facilities interdependencies are addressed appropriately.

Management's Response: NASA partially concurs with this recommendation. The Principal Advisor for Enterprise Protection will establish and enhance, through the ICSWG discussed in Recommendation 2, an integrated functional review process focused on protecting strategically critical capabilities and technologies in order to ensure cyber, facility, and mission interdependencies are addressed appropriately and to reduce the overall burden on the missions and facilities operations.

Estimated Completion Date: October 1, 2018

Recommendation 4: The Assistant Administrators of OPS and OSI, in conjunction with the Agency Chief Information Officer, coordinate the development of a methodology for the identification and protection of interdependencies (either within the facility security assessment or facility security level designation process).

Management's Response: NASA partially concurs with this recommendation. NASA concurs with the intent of this recommendation, but not with the recommended implementation. The Principal Advisor for Enterprise Protection will establish an ICSWG, as discussed in Recommendation 2, to include OPS, OSI, and OCIO, to coordinate the development of a methodology for the identification and protection of interdependencies.

Estimated Completion Date: October 1, 2018

Recommendation 5: The Agency Chief Information Officer, in conjunction with the Assistant Administrators of OPS and OSI, develop security policy based on NIST SP 800-53, rev. 4 and NIST SP 800-82 guidance for managing the protection of OT within the mission and institutional directorates. At a minimum, this should include:

a. defining control systems;

b. identifying all OT systems at NASA and a strategy for segmenting OT from Information Technology (IT) across the Agency;

c. utilizing Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) alerts when assessing control systems security posture;

d. developing system security plans and assessment methodologies for control systems/OT in a way that ensures the use of appropriate system boundaries

and effective compensating controls, in the absence of common controls or automation as defined in NIST SP 800-82; and

e. developing training for responsible security personnel in line with NIST and Department of Homeland Security (DHS) guidance on control system security. This may include control system administrators, OCIO approval authorities, control system owners, and assessment teams.

Management's Response: NASA partially concurs with this recommendation. NASA concurs with the intent of this recommendation, but not with the recommended implementation. The Principal Advisor for Enterprise Protection will establish a coordinated process through the ICSWG, as discussed in Recommendation 2, to coordinate the development of a security policy based on NIST SP 800-53, rev. 4 and NIST SP 800-82 guidance for managing the protection of OT within the mission and institutional directorates. At a minimum, this shall include:

a. defining control systems;

b. identifying all OT systems at NASA and a strategy for segmenting OT from IT across the Agency;

c. utilizing ICS-CERT alerts when assessing control systems security posture;

d. developing system security plans and assessment methodologies for OT in a way that ensures the use of appropriate system boundaries and effective compensating controls, in the absence of common controls or automation as defined in NIST SP 800-82, revision 2; and

e. developing training for responsible security personnel in line with NIST and DHS guidance on control system security. This may include control system administrators, OCIO approval authorities, control system owners, and assessment teams.

Estimated Completion Date: October 1, 2018

Recommendation 6: Establish an integrated cyber and physical risk management committee or oversight body composed of subject matter experts from NASA Mission Directorates, OCIO, OPS, and OSI.

Management's Response: NASA concurs with this recommendation. NASA has established an EPP that is coordinated through the EPB. The EPB consists of the Associate Administrators from each of the mission directorates as well as the Chief's from the mission support offices. The EPB is advisory and will integrate recommendations into, where practical, existing cyber, space, aeronautic, institutional, national security, and mission protection working groups and policies.

The EPP and EPB are chartered under the authority of the Agency Program Management Council.

Estimated Completion Date: Completed

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 Mr. James Leatherwood (202) 358-3608.

James Leatherwood
Principal Advisor
NASA Enterprise Protection

cc:
Acting Administrator/Mr. Lightfoot
Deputy Associate Administrator/Ms. Roe
Human Exploration and Operations Mission Directorate/Mr. Gerstenmaier
Office of Protective Services/Mr. Mahaley
Mission Support Directorate/Ms. Paquin
Office of the Chief Engineer/Mr. Roe
Aeronautics Research Mission Directorate/Mr. Shin
Office of the Chief Information Officer/Ms. Wynn
Office of Strategic Infrastructure/Mr. Williams
Office of Safety and Mission Assurance/Mr. Wilcutt
Science Mission Directorate/Mr. Zurbuchen

APPENDIX D: REPORT DISTRIBUTION

National Aeronautics and Space Administration

Acting Administrator
Acting Deputy Administrator
Acting Chief of Staff
Chief Information Officer
Associate Administrator, Mission Support
Assistant Administrator, Office of Protective Services
Assistant Administrator, Office of Strategic Infrastructure
Principal Advisor for Enterprise Protection

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-16-001-00)