NASA

National Aeronautics and Space Administration

Office of Inspector General

Office of Audits

NASA'S INSIDER THREAT PROGRAM

March 14, 2022

Report No. IG-22-009

Office of Inspector General

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

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

NASA Office of Inspector General
Office of Audits

RESULTS IN BRIEF

NASA's Insider Threat Program

March 14, 2022 IG-22-009 (A-21-013-00-MSD)

WHY WE PERFORMED THIS AUDIT

Cybersecurity threats posed by an organization's employees and contractors are commonly referred to as insider threats. Insiders typically fly under the radar of traditional security defenses, making it difficult to detect and prevent any improper activities. According to government and industry experts, the most common insider threats arise from:

- accidental leaks, which might originate from a phishing attack or from an employee forwarding a sensitive email to the wrong person;
- misuse of network access or database privileges, where an employee intentionally circumvents cybersecurity policies or procedures; and
- data theft, where an employee removes data from an organization with the intent of selling or otherwise inappropriately releasing it.

Given NASA's high-profile mission and broad connectivity with educational institutions, research facilities, and international partners, its risk exposure from insider threats is significant and varied. In this audit, we examined whether NASA has implemented an effective insider threat program in accordance with federal and Agency policies and cybersecurity leading practices. Specifically, we examined whether: (1) NASA's insider threat strategy provides an adequate framework for identifying malicious and unintentional insider threats; (2) NASA implemented appropriate procurement controls to identify and prevent intellectual data theft from foreign adversaries, and (3) NASA developed adequate cybersecurity controls to prevent, detect, and respond to the extraction or manipulation of data and intellectual property. To conduct our work, we reviewed federal and Agency policies, regulations, and guidance, as well as industry best practices; interviewed numerous NASA officials from the Office of Protective Services, Office of Chief Information Officer, and Office of Procurement; and met with the National Insider Threat Task Force.

WHAT WE FOUND

NASA, like all federal agencies, is required to address insider threats on its *classified* systems, and we found the Agency has taken appropriate steps to implement an insider threat program for those systems. Specifically, we determined that NASA established user activity monitoring, developed mandatory Agency-wide insider threat training, and created an insider threat reference website that assists employees and contractors with identifying threats, risks, and follow-up information. Additionally, the Agency is strengthening procurement controls by expanding disclosure requirements and updating procedures to address the risks of foreign influence.

While NASA has a fully operational insider threat program for its *classified* systems, the vast majority of the Agency's information technology (IT) systems—including many containing high-value assets or critical infrastructure—are *unclassified* and are therefore not covered by its current insider threat program. Consequently, the Agency may be facing a higher-than-necessary risk to its unclassified systems and data. While NASA's exclusion of unclassified systems from its insider threat program is common among federal agencies, adding those systems to a multi-faceted security program could provide an additional level of maturity to the program and better protect agency resources. According to

Agency officials, expanding the insider threat program to unclassified systems would benefit the Agency's cybersecurity posture if incremental improvements, such as focusing on IT systems and people at the most risk, were implemented. However, on-going concerns including staffing challenges, technology resource limitations, and lack of funding to support such an expansion would need to be addressed prior to enhancing the existing program.

Further amplifying the complexities of insider threats are the cross-discipline challenges surrounding cybersecurity expertise. At NASA, responsibilities for unclassified systems are largely shared between the Office of Protective Services and the Office of the Chief Information Officer. In addition, Agency contracts are managed by the Office of Procurement while grants and cooperative agreements are managed by the Office of the Chief Financial Officer. Nonetheless, in our view, mitigating the risk of an insider threat is a team sport in which a comprehensive insider threat risk assessment would allow the Agency to gather key information on weak spots or gaps in administrative processes and cybersecurity. At a time when there is growing concern about the continuing threats of foreign influence, taking the proactive step to conduct a risk assessment to evaluate NASA's unclassified systems ensures that gaps cannot be exploited in ways that undermine the Agency's ability to carry out its mission.

WHAT WE RECOMMENDED

In order to strengthen NASA's insider threat program, we recommended the Associate Administrator, Assistant Administrator for Protective Services, and the Chief Information Officer:

1. Establish a cross-discipline team to conduct an insider threat risk assessment to evaluate NASA's unclassified systems and determine if the corresponding risk warrants expansion of the insider threat program to include these systems.

2. Improve cross-discipline communication by establishing a Working Group that includes the Office of Protective Services (OPS), the Office of the Chief Information Officer (OCIO), the Office of Procurement, human resources officials, and any other relevant Agency offices to collaborate on wide-ranging insider threat related issues for both classified and unclassified systems.

We provided a draft of this report to NASA management who concurred with our recommendations. We consider management's comments responsive; therefore, the 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

CISA	Cybersecurity and Infrastructure Security Agency
CUI	Controlled Unclassified Information
GAO	Government Accountability Office
IT	information technology
NIST	National Institute of Standards and Technology
NITTF	National Insider Threat Task Force
OCFO	Office of the Chief Financial Officer
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OPS	Office of Protective Services
SBU	Sensitive but Unclassified

INTRODUCTION

Cybersecurity threats to information technology (networks, systems, and data) posed by an organization's own employees and contractors are commonly referred to as insider threats. Importantly, when insiders misuse their authorized access to sensitive data or systems the organization is negatively impacted. With people as the primary attack vector, an insider threat program is far more than a technical program.[1] Insiders typically fly under the radar of traditional security defenses, making it difficult to detect and prevent their actions. Consequently, detecting those threats is one of the biggest challenges that cybersecurity programs face. According to government and industry standards, the most common insider threats arise from:

- accidental leaks, which might originate from a phishing attack or from an employee forwarding a sensitive email to the wrong person;
- misuse of network access or database privileges access, where an employee intentionally circumvents cybersecurity policies or procedures; and
- data theft, where an employee removes data from an organization with the intent of selling the data or otherwise inappropriately releasing it.

NASA, like all federal agencies, is required to address insider threats on its classified systems.[2] Given the Agency's high-profile mission and broad connectivity with educational institutions, research facilities, and international partners, NASA's risk exposure from insider threats is significant and varied. In this audit, we examined whether NASA has implemented an effective insider threat program in accordance with federal policies, its own Agency policies, and cybersecurity leading practices. Specifically, we examined whether: (1) NASA's insider threat strategy provides an adequate framework for identifying malicious and unintentional insider threats; (2) NASA implemented appropriate procurement controls to identify and prevent intellectual data theft from foreign adversaries, and (3) NASA developed adequate cybersecurity controls to prevent, detect, and respond to the extraction or manipulation of data and intellectual property. For details on our scope and methodology, please see Appendix A.

[1] In cybersecurity, an attack vector is a path or means by which an attacker gains unauthorized access to a computer or network, for example, through email, websites, or social engineering.

[2] Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information* (October 2011).

Background

An insider threat is often hidden in plain sight, with the perpetrator posing a substantial threat by virtue of their knowledge of and access to the organization's information technology (IT) systems and databases. Insider threats are people—employees, former employees, contractors, business partners, or vendors—with legitimate access to an organization's networks and systems. In the context of safeguarding their assets, organizations have to be on guard against both unwitting and witting insiders.

Insider Threats

Unwitting Insider. An employee who has made an honest mistake. For example, the person could send an email containing sensitive information to the wrong person, email sensitive company data to personal accounts to conduct work over the weekend, fall victim to a phishing attack, or lose their work-issued phone or computer.

Witting Insider. A malicious actor who intentionally steals data. For example, the person might exfiltrate valuable information such as intellectual property, personally identifiable information (e.g., social security number or date of birth) for financial incentive, a competitive edge, or as retribution when they believe they have been treated unfairly by the organization.

Federal agencies and commercial organizations must take an enterprise-wide approach to properly plan for, prevent, detect, respond to, and recover from insider threats. While technology plays a vital role in identifying potential insider threats, the issue extends beyond IT management. Leading practices indicate that insider threat risk management should be part of a holistic security program and should incorporate information security, physical security, human resources, procurement controls, and workforce training. As shown in Table 1, private sector industry trends indicate insider threats are intensifying.

Table 1: Private Sector Insider Threats by the Numbers

Source: OIG presentation of industry data, https://bit.ly/3qDIMea (last accessed January 7, 2022).

An effective cybersecurity program is profoundly difficult to manage, especially in an ever-changing threat environment where mitigation is a marathon, not a sprint. We have identified NASA's ongoing efforts to stem cyberattacks and secure its IT systems as a top management challenge for almost 20 years. As attackers become more aggressive, organized, and sophisticated, managing and mitigating cybersecurity risk is critical to protecting NASA's vast network of IT systems from malicious attacks or insider threats that can seriously impede the Agency's ability to carry out its mission.

NASA's insider threat program, established in 2014, is housed within the Office of Protective Services and staffed by one full-time government employee and two contract employees supporting user activity monitoring. The program is solely focused on compliance with Executive Order 13587 to address insider threats related to classified systems and does not address similar risks to unclassified systems—which make up the vast majority of NASA's IT systems. In addition to staffing, the program has procured software to monitor the classified network for anomalous user activity.

Collaboration and Competition in Space

NASA strives to inspire Americans and share the excitement of space by providing "for the widest practicable and appropriate dissemination of information concerning its activities and the results thereof."[3] To that end, the Agency takes an open, collaborative approach to data sharing: for example, NASA publicly shares data on active fires, flooding projections, and weather modeling. Similarly, the Agency's approach to human space exploration is largely collaborative. The International Space Station, for example, has been operating in low Earth orbit for more than 20 years; its structure and modules include contributions from NASA, the Russian Space Agency Roscosmos, the European Space Agency, the Japan Aerospace Exploration Agency, and the Canadian Space Agency. In addition, 240 people from 19 countries have served on its crew.[4]

Competition is also a driver of humankind's endeavors in space. NASA Administrator Bill Nelson recently noted that "China's successful rover landing on Mars is a warning to the U.S. government that the space agency faces stiff competition in the future."[5] Additionally, according to the United Nations Office for Outer Space Affairs, the number of space faring nations continues to increase, all at varying degrees of development.[6]

Moreover, an increasingly competitive and burgeoning commercial space industry accomplished 135 successful orbital space launches in 2021—the most ever. The world witnessed more than a dozen private citizens reach the edges of space on commercial spaceflight ventures, China bring back samples from the moon, NASA launch the James Webb Telescope on Christmas Day, and Russia launch a new robotic cargo ship to the International Space Station. Notably, China edged out the U.S. for the most missions by any country with 53 (the U.S. and Russia followed with 48 and 24, respectively).

---

[3] National Aeronautics and Space Act of 1958 as recodified and amended at 51 U.S.C. § 20112(a)(3).

[4] *Celebrating 20 Years of Human Presence on the ISS*, https://www.nasa.gov/sites/default/files/atoms/files/iss20_celebrating_20_years.pdf (last accessed January 25, 2022).

[5] *NASA Boss Bill Nelson Says China 'Aggressive Competitor' After Mars Landing*, May 20, 2021, https://www.newsweek.com/nasa-bill-nelson-china-competitor-mars-rover-moon-landings-planning-1593241 (last accessed January 7, 2022).

[6] *United Nations Office for Outer Space Affairs, World Space Agencies Web Page,* https://www.unoosa.org/oosa/en/ourwork/space-agencies.html (last accessed January 7, 2022).

This tension between collaboration and competition will continue to be an aspect of space activities in the coming years. At NASA, both collaborative and competitive international relationships need to be continually evaluated through the lens of cyber risk. Numerous geopolitical factors have the potential to affect the balance of the Agency's cyber posture, such as:

- Collaborating with other countries can at times put the United States' technological advantage at risk, jeopardizing intellectual property and potentially compromising national security. The United States Trade Representative's priority watch list for Intellectual Property Protection includes Argentina, Chile, China, India, Indonesia, Russia, Saudi Arabia, Ukraine, and Venezuela —all countries with space programs.
- The U.S. limits the export of certain technologies and information, including the transfer of intellectual knowledge to individuals from countries listed on the trade priority watch list. For example, NASA is prohibited by law from using government funds to cooperate with the Chinese bilaterally in space.[7] According to the Department of Justice, a Chinese nexus exists in around 60 percent of all trade secret theft cases. In addition, Russian state actors are known to use hacking, espionage, and cyberattacks to steal U.S. defense and trade secrets.
- Space technology often has potential uses in both commercial and military settings. The Department of Commerce has listed telecommunications technologies and information security as falling into this category, which it characterizes as "dual-use items."[8]

Insider Threats from Foreign Government Recruitment Programs

Several countries seek to illegally acquire U.S. technology from U.S.-based scientists and academics. Nations such as Russia and Iran wage sophisticated cyber espionage campaigns directed at the acquisition of U.S. trade secrets in both the private and government sectors, while other countries like China attempt to blur the line between informal technology transfer and intellectual property theft by recruiting leading U.S. experts in high-tech fields. Currently, China is by far the most prolific sponsor of such recruitment programs through what it calls "Talent Plans." According to the Federal Bureau of Investigation (FBI), the U.S. is a priority target for China's talent plan recruitment efforts given the U.S. leadership in key technology fields such as nuclear energy, wind tunnel design, telecommunications, and advanced lasers.[9] China's national and local government entities oversee hundreds of talent plans designed to acquire foreign technologies. Through covert cyber intrusions, bad actors gain unauthorized access to a wide range of commercially valuable U.S. business information—including intellectual property, trade secrets, technical data, negotiating positions, and sensitive and proprietary internal communications—which are then provided to and utilized by foreign firms.

While sometimes presented as international collaboration opportunities, talent plans often create a one-way transfer of technology and expertise to the detriment of U.S. agencies, businesses, and

---

[7] Public law 112-10, *Department of Defense and Full-Year Continuing Appropriations Act, 2011*, April 15, 2011, Sec 1340 (often referred to as the Wolf amendment) prohibits NASA from participating, collaborating, or coordinating with China or any Chinese owned company.

[8] 15 CFR Appendix Supplement No. 1 to Part 774 - *The Commerce Control List* (August 19, 2021).

[9] FBI Public Service Announcement, *Foreign Government-Sponsored Talent Recruitment Plans, such as China's Talent Plans, Incentivize Economic Espionage and Theft of Trade Secrets* (#20200716-2, July 16, 2020), https://www.fbi.gov/investigate/counterintelligence/the-china-threat/chinese-talent-plans (last accessed January 7, 2022).

universities. For example, Chinese talent plan members agree to be subject to China's laws, including those related to national security, intellectual property, and secrecy, which effectively prohibit the individual from sharing new technology developments or research breakthroughs with their U.S. employer or funding agency without special authorization from China's government, undermining the common standard of reciprocity of research. In addition, plan participants are often contractually required to recruit other experts into the talent plan community. Such a requirement may create further risk to the talent plan participant's U.S. employer given the participants' proximity to co-workers and sensitive competitive information.

NASA Cases

NASA routinely hosts and partners with international students, scholars, and researchers, which complicates the Agency's insider threat exposure. Recently, multiple professors and researchers at American universities have been arrested on charges related to lying about or failing to disclose their ties with foreign governments while accepting NASA-funded grants. This is a hallmark of China's targeting of research and academic collaborations in order to obtain U.S. technology. For example:

- In June 2021, a senior NASA scientist holding a trusted position with access to valuable intellectual property was sentenced to 30 days in prison and fined $100,000 after pleading guilty to making false statements related to Chinese Thousand Talents Program. Investigators found that over an almost 8-year period, the scientist provided Chinese researchers with data, documents, and guidance on biosensors; assisted them with nanodevice fabrication; helped a Chinese company manufacture a smartphone sensor akin to NASA's design; and provided Chinese nationals with access to NASA facilities.[10] The scientist received an estimated $1.4 million over five years for working as a visiting professor at Soochow University in China.
- In August 2020, a Texas A&M University researcher was arrested for conspiracy and fraud over his relationship with a number of Chinese universities while receiving grants from NASA. According to the criminal complaint filed by the FBI, the researcher engaged in a seven-year scheme to gain access to "the unique resources of the International Space Station," to leverage NASA grant resources for Chinese institutions and to enrich himself by $86,876.
- In July 2020, a professor and researcher working with NASA on proprietary research at the University of Arkansas High-Density Electronics Center was indicted after failing to disclose his ties to Chinese universities and companies while accepting NASA grant funding.

Federal Guidance

Executive Order 13587, issued in October 2011, requires federal agencies to create insider threat programs to protect classified information and implement guidelines and standards developed by the Office of the Director of National Intelligence's National Insider Threat Task Force.[11] This order mandates structural reforms across the government to ensure responsible sharing and safeguarding of *classified* information on computer networks.

[10] A biosensor is comprised of a biological sensing element and a physical transducer that converts the recognition phenomenon into a measurable signal. A nanodevice is comprised of one or more nanoscale components essential to its operation.

[11] Executive Order 13587.

In November 2012, the President released a memorandum transmitting the National Insider Threat Policy and minimum standards for Executive Branch Insider Threat Programs, which focused on strengthening and safeguarding federal efforts to counter insiders who may use their authorized access to compromise sensitive information.[12] The policy incorporated requirements from Executive Order 13587 to develop insider threat detection and prevention programs. The National Insider Threat Policy established 26 minimum standards for insider threat programs at executive branch agencies. Agencies are required to implement these minimum standards before they can be designated as having full operating capability. The National Insider Threat Task Force designates insider threat programs as having achieved full operating capability when programs, among other things:

- operate in a proactive posture;
- receive strong and active support from the agency head;
- designate a senior official with direct access to the agency head to discuss insider threat matters;
- have access to multiple internal and external data sources to help with insider threat detection and prevention; and
- create a culture of awareness about insider threats.

In April 2013, the National Institute of Standards and Technology (NIST) issued a publication stating that the standards and guidelines that apply to insider threat programs in *classified* environments can also be employed effectively to improve the security of *unclassified* information in non-national security systems.[13] Specifically, the NIST publication states that an effective insider threat program needs: formal policies and implementation plans; host-based monitoring of employee activities; a cross-discipline team and security controls aimed at detecting and preventing malicious insider activity; employee awareness training; self-assessments of compliance with insider threat policies; and legal support to ensure monitoring is in accordance with laws and regulations.[14]

The NIST publication also highlights the importance for the cross-discipline team to have access to information from all relevant offices (e.g., human resources, legal, physical security, personnel security, IT, information system security, and law enforcement). Human resource records are especially important for insider threat analysis; for example, such records may reveal patterns of disgruntled behavior and conflicts with coworkers and other colleagues. Further discussion of insider threat behavioral indicators can be found in Appendix C.

[12] *National Insider Threat Policy and Minimum Standards*, November 2012; The National Insider Threat Task Force operates within the Office of the Director of National Intelligence.

[13] National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013).

[14] Broadly, classified systems contain information that must be protected in the interest of national security to prevent adversaries from gaining insight into sensitive information, activities, technology, or intellectual property. Examples include information or data related to national defense, foreign relations, or system capabilities.

Procurement Management

NASA uses contracts, grants, and cooperative agreements to obtain goods and services in support of its mission.[15] Through these procurement vehicles, tens of thousands of NASA employees and contractors are given access to non-public NASA networks, systems, and facilities, increasing the possibility that individuals and organizations might improperly access Agency data.

While the Office of Protective Services is responsible for vetting incoming contractors and researchers that will have access to NASA systems and facilities, both the Office of Procurement (Procurement) and the Office of the Chief Financial Officer (OCFO) play a role in NASA's insider threat protection efforts.

- Procurement focuses on supply chain management, ensuring that appropriate clauses such as those prohibiting the use of covered IT telecommunications equipment from China, are included in its contracts.[16] Additionally, Procurement works with the Office of General Counsel and the Space Technology Mission Directorate to ensure intellectual property protections are included in contracts.
- OCFO focuses on ensuring appropriate disclosure requirements for key members of research teams are included in grant and cooperative agreements.[17] Federal agencies that fund research have a strong interest in ensuring research is scientifically rigorous and free of bias, including foreign influence. To avoid conflicts of interest associated with federal awards and to address foreign interest concerns, NASA requires researchers to disclose conflict of interest information about their affiliations, associations, and activities, such as any current or pending financial support; this may also indicate potential non-financial conflicts, such as the same research being supported by other federal agencies or a foreign government.[18]

[15] A contract is an agreement between parties creating mutual obligations enforceable by law. A grant is federal financial assistance provided by the government that funds projects to provide public services. A cooperative agreement is a type of grant where there is substantial involvement from both the federal agency and the awardee.

[16] Covered telecommunications equipment or services means telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities).

[17] Presidential Memorandum on United States Government - *Supported Research and Development National Security Policy* (January 14, 2021).

[18] Conflict of interest policies protect the integrity of U.S. research against the influence of the researcher's financial interests on the design, conduct, and reporting of the results of federally funded research.

NASA IS ADDRESSING INSIDER THREATS FOR ITS CLASSIFIED SYSTEMS, YET RISKS PERSIST FOR UNCLASSIFIED SYSTEMS

NASA has taken appropriate steps to implement an insider threat program that meets federal requirements for its *classified* systems. Specifically, we determined that NASA established user activity monitoring, developed mandatory Agency-wide insider threat training, and created an insider threat reference website that assists employees and contractors with identifying threats, their risks, and follow-up information. Additionally, the Agency is strengthening procurement controls by expanding disclosure requirements and updating procedures to address risks of foreign influence. While NASA has a fully operational insider threat program for its *classified* systems, the vast majority of its IT systems—including many containing high-value assets and critical infrastructure—are *unclassified* and are therefore not covered by its current insider threat program. Consequently, the Agency may be facing a higher-than-necessary risk to its unclassified systems and data.

NASA's Insider Threat Program Meets Requirements for Classified Systems

NASA established its insider threat program in October 2014 to meet federal requirements and designated the Assistant Administrator for Protective Services as the Agency's insider threat senior official. [19] The Agency-wide initiative seeks to:

- Enhance the safety and security of NASA's classified computer networks by establishing an integrated capability to monitor and audit user activity across all *classified* domains to detect and mitigate activity indicative of insider threat behavior;[20]
- Facilitate the sharing of counterintelligence, security, information assurance, law enforcement, human resources, and other related information to recognize and counter the presence of an insider threat;
- Evaluate personnel security information for possible insider threat behaviors;
- Provide the NASA workforce with training on the insider threat, counterintelligence awareness, and their reporting responsibilities;
- Gather information to establish a centralized, analysis, reporting, and response capability;
- Utilize risk management principles and definitions accepted across the federal government and private industry, tailored to meet the distinct needs of NASA missions and programs; and

[19] Executive Order 13587.

[20] NASA Policy Directive 1600.9A, *NASA Insider Threat Program*, September 2021, mirrors federal requirements and incorporates insider threat and counterintelligence awareness training within 30-days of initial employment.

- Include appropriate protections for privacy.

In November 2018, the National Insider Threat Task Force (NITTF) designated NASA's insider threat program as having full operating capability, certifying that the program had successfully implemented its 26 minimum standards for insider threat programs at executive branch agencies.[21] Since receiving that designation, NASA's program has focused primarily on developing annual mandatory Agency-wide insider threat training, establishing user activity monitoring, and standing up a reference website that provides tools and resources to help the workforce understand how everyone plays a part in protecting data and programs from insider threats.

NASA's Insider Threat Program is Proactive

Both the federal government and private sector organizations such as the National Insider Threat Task Force, Cybersecurity and Infrastructure Security Agency, National Institute of Standards and Technology (NIST), and Carnegie Mellon University have developed extensive guidance to help mitigate insider threats.[22] In particular, the NITTF has produced a number of standards, advisories, guides, and bulletins to help organizations build effective insider threat programs. NITTF's maturity framework aids agencies in advancing their programs beyond the minimum standards and helps insider threat programs become more proactive, comprehensive, and better postured to deter, detect, and mitigate insider threat risk. Additionally, external resources such as the "Insider Threat Program Maturity Model" provide organizations with a way to benchmark their current insider threat risk posture and determine a path to further mature their existing program.[23] See Appendix B for additional details on the Insider Threat Maturity Model. NIST has also contributed to the field and has a library of wide-ranging documents to assist government and private sector organizations in assessing and managing risks, including insider threats.[24] Collectively, these publications provide a framework of security and privacy controls needed to protect critical infrastructure from threats like hostile attacks, human error, and malign foreign intelligence activities.

Using the Insider Threat Program Maturity Model, shown in Table 2 below, we rated NASA's insider threat program for classified systems as being *proactive*.

[21] Achieving full operating capability certification from the National Insider Threat Task Force is a one-time occurrence.

[22] Carnegie Mellon University has a library of educational instruction widely available for managing insider threats from both witting and unwitting insiders, https://www.sei.cmu.edu/publications/technical-papers/index.cfm (last accessed January 7, 2022).

[23] The Insider Threat Maturity Model, adapted from government, academia, and industry best practices, was authored by Jim Henderson, CEO of Insider Threat Defense, and Nick Cavalancia, Founder & Chief Techvangelist at Techvangelism, to help security professionals assess their organization's ability to monitor for, detect, and respond to insider threats, https://bit.ly/32ROOQ8 (last accessed January 7, 2022).

[24] NIST Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* (September 2020); NIST SP 800-30, Rev. 1, *Guide for Conducting Risk Assessments* (September 2012); and NIST SP 800-37, Rev. 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* (December 2018).

Table 2: Insider Threat Program Maturity Model

Maturity Level	Definition
Nonexistent	The organization has no program or technology in place to detect and respond to insider threats and is unaware of the risk posed by an insider threat.
Reactive	The organization has no program in place but is aware that insider threats exist. IT is responsible for responding to any realized threat actions.
Proactive	***The organization's focus is on the use of technologies (and the necessary interdepartmental communication to facilitate use) that will help spot any insider threats within a core group of high-risk users.***
Predictive	The organization has a formal program in place that seeks to identify potential or active threats as early as possible. Program definitions, policies, processes, and technologies are in place organization wide.
Optimized	The organization's program is holistic, dynamic, and responsive, continually addressing shifting risk and changes in business operations that impact needed policy, process, and technologies.

Source: OIG analysis based on the *Insider Threat Program Maturity Model Report*, January 22, 2019, https://bit.ly/32ROOQ8 (last accessed January 7, 2022).

In our judgement, the maturity of NASA's *classified* insider threat program is generally adequate for preventing significant harm to its systems from both unwitting and witting insiders. By implementing all 26 of the NITTF minimum standards and focusing on user activity monitoring through log collection and analysis, NASA made positive progress in the development of its insider threat program. Importantly, in conjunction with general IT security training, NASA mandates annual insider threat awareness training for all civil servants and contractors with a security clearance.[25] Developed by the NITTF, the course covers topics such as adversaries, behavioral indicators, and reporting requirements. In our opinion, training courses are effective at inhibiting unwitting insider negligence by identifying best practices and encouraging employee vigilance. Indeed, annual web-based training bolsters security awareness without imposing significant costs on the Agency.

We also found NASA's program is effectively designed to monitor the classified network for anomalous user activity. Further, the Agency's insider threat program is supported by ad hoc interdepartmental communication between Office of Protective Services divisions such as Personnel Security, the Intelligence Division, and Physical Security; such communication is important for helping NASA identify and mitigate threats.

At the same time, not all damaging cyber events are *classified* in nature, so another key to NASA's overall insider threat security program is the ability to identify the impact of an unclassified damaging event, should it occur. A benchmarking resource, such as the Insider Threat Program Maturity Model, would assist the Agency by highlighting other critical assets needing protection from insider harm.

[25] The System for Administration, Training, and Educational Resources for NASA (SATERN) is NASA's Learning Management System that provides web-based training including courses on insider threats.

Vast Majority of NASA's Systems are Unclassified

While federal requirements to date have focused on protecting an agency's *classified* systems, the insider threat to *unclassified* systems is significant given that the overwhelming majority of systems at NASA are unclassified and many contain sensitive and valuable information such as scientific, engineering, or research data; human resources files; or procurement sensitive information. The NITTF suggests that efforts to mitigate insider threats must include protection of an organization's "crown jewels." At NASA, valuable data including information related to critical infrastructure and other high-value assets resides in unclassified systems.[26] Consequently, an insider threat incident on an unclassified system could pose serious jeopardy to Agency operations.

NASA limits physical access to high-value assets and critical infrastructure but does not specifically monitor access to unclassified data pertaining to intellectual property and high-value assets. Agency-owned unclassified computer systems are initially assigned to users with limited privileges; however, due to the Agency's role in the research and scientific communities, a large number of individuals typically require elevated privileges so that they can download task-specific software.[27] For instance, within the last three years NASA users have made over 12,000 requests for elevated privileges. Without proper monitoring of the purpose and source of this software, NASA systems are vulnerable to the introduction of malicious artifacts that can sabotage systems or collect and deliver information to outside sources. Additionally, accessing IT systems with elevated user privileges greatly increases the risks of cybersecurity incidents by introducing unintended, detrimental changes to system configurations. For example, a user accessing a computer with elevated privileges has the ability to access, alter, and delete critical data; exploit bugs; or exploit design flaws.

Although malicious insiders are a significant danger to any organization, many insider threats are the result of simple human error. For example, an unwitting insider might click on a link that leads to a phishing attack or accidentally send a confidential email to the wrong recipient. In a May 2021 report, we found that incidents of improper use of NASA IT systems had increased from 249 in 2017 to 1,103 in 2020—a 343 percent growth; the most prevalent error was failing to protect Sensitive but Unclassified (SBU) information.[28] An example of this would be sending unencrypted email containing SBU data, Personally Identifiable Information, or International Traffic in Arms Regulations data, any of which could expose the Agency to a risk that can affect national security, incur a loss of intellectual property, or compromise sensitive employee and contractor data.[29]

---

[26] High-Value Assets, colloquially called "crown jewels," is information or an information system so critical to an organization that the loss or corruption of this information or loss of access to the system would have serious impact to the organization's ability to perform its mission or conduct business. These sensitivities make High-Value Assets of particular interest to criminal, politically motivated, or state-sponsored actors for either direct exploitation of the data or a spill that would cause a loss of public confidence.

[27] The principle of "least privilege" instructs that access rights for users should be restricted to those resources minimally required to perform legitimate activities.

[28] NASA OIG, *NASA's Cybersecurity Readiness* (IG-21-019, May 18, 2021). Sensitive but Unclassified has been replaced by a newly mandated government-wide initiative and renamed as Controlled Unclassified Information. NASA was issued a waiver that permitted both information classifications to coexist until October 1, 2021.

[29] Personally Identifiable Information is any data, such as a social security number or date of birth, that could potentially identify a specific individual. International Traffic in Arms Regulations (ITAR) control the export and import of defense-related articles and services on the United States Munitions List and affects the manufacture, sale, and distribution of technology.

Insider Threats to Unclassified Systems Remain Important to Evaluate

Although the Agency has implemented countermeasures to reduce the risk of insider threats to *classified* systems, it continues to face challenges in improving its defenses to protect unclassified systems. While excluding unclassified systems from the insider threat program is not unique to NASA among federal agencies, adding those systems could provide an additional level of maturity to the program and better protect agency resources. Notably, some federal agencies are expanding their insider threat programs to include unclassified systems. For example, in 2020 the Tennessee Valley Authority chose to implement its insider threat program to include both classified and unclassified systems to protect personnel, facilities, information systems, and the information within such systems.[30] Likewise, the Department of Defense (DoD) and the Department of Homeland Security (DHS) have begun to include unclassified systems in their insider risk programs. The expanded scope at DoD and DHS increases the population covered to include anyone—past or present—with access to agency facilities, information, equipment, networks, or systems.

As the threat landscape continues to expand, so too must insider threat program strategies, procedures, and supporting technologies. A comprehensive insider threat program must consider new and increased stressors on employees experienced during the COVID-19 pandemic, the growing reach and sophistication of technical and social strategies of adversaries, the expanding reach of acts of economic espionage, and expanded vulnerabilities inherent to having extremely large numbers of teleworkers. A formal evaluation of the costs and operational requirements of mitigating the insider threat risk to unclassified systems would help NASA obtain a full picture of its cyber risk exposure and better secure its intellectual property.

According to NASA OPS officials, expanding the insider threat program to unclassified systems would benefit the Agency's cybersecurity posture if incremental improvements, such as focusing on IT systems and people at the most risk, were implemented. Nevertheless, officials expressed on-going concerns such as staffing challenges, technology resource limitations, and lack of funding to support such an effort that would need to be addressed prior to enhancing the existing program. While we agree these are valid concerns, given that unclassified systems constitute the vast majority of IT systems at NASA, expansion of the Agency's insider threat program is important to consider.

Responsibility for Insider Threat Protection is Split between Several Offices

Further amplifying the complexities of insider threats are the cross-discipline challenges surrounding cybersecurity expertise. At NASA, responsibilities for unclassified systems are largely shared between OPS and the Office of the Chief Information Officer (OCIO). For example, although OPS is currently responsible for managing the Agency's insider threat program for classified systems, as required under the Executive Order, its capabilities for expanding monitoring to unclassified systems would be constrained due to manpower, funding, and technological limitations. Conversely, the OCIO has the cybersecurity staff and capabilities to monitor the Agency's network for data loss prevention and behavioral analysis but has no defined responsibility to monitor unclassified systems for indicators of compromise specifically related to insider threats. In addition to the fragmented responsibilities

[30] TVA OIG Audit Report, *Insider Threat Program*, April 29, 2020, https://oig.tva.gov/reports/20rpts/2019-15619.pdf.

between OPS and OCIO, Agency contracts are managed by Procurement while grants and cooperative agreements are issued by the NASA Shared Services Center and managed by the OCFO.

In our view, cross-discipline challenges need to be reviewed and evaluated to identify the best approach for mitigating potential insider threats to unclassified systems. Although the Agency's insider threat program is supported by ad hoc communication between various OPS divisions such as Personnel Security and Intelligence, there is no consistent collaboration across organizations to proactively assess insider threat risk to its unclassified systems. Mitigating the risk of an insider threat is a team sport; a comprehensive insider threat risk assessment by offices such as human resources, legal, and IT would allow the Agency to gather key information on weak spots or gaps in administrative processes and cybersecurity. Collectively, this cross-discipline team could evaluate the consequences of potential security incidents. Such information could then be used to determine relevant cybersecurity improvements to prevent, detect, and respond to insider threats. Ultimately, NASA needs to ensure that all offices with a role in insider threat protection are sharing information with one another in order to protect against insider threats.

Procurement Policy Updates Pending

NASA is strengthening procurement controls by expanding disclosure requirements for its grants and cooperative agreements and updating procedures to address risks of foreign influence as a result of recent reports by the Government Accountability Office (GAO), the Senate Homeland Security and Government Affairs committee, and White House guidance identifying challenges facing the research community.[31] For example, the OCFO is updating NASA's conflict of interest policy to address undue foreign influence while maintaining an open research environment that fosters collaboration, transparency, and the free exchange of ideas.

In particular, a 2020 GAO report found that agencies need to enhance policies to address foreign influence and examine the extent to which research-supporting agencies identify and mitigate foreign influence in research.[32] The report includes two recommendations for NASA, specifically (1) updating the Agency's conflict of interest policy to include a definition on non-financial conflicts and address these conflicts, and (2) documenting procedures, including roles and responsibilities for addressing and enforcing failures to disclose required information, both foreign and domestic.

Similarly, the Senate report determined that, "while China has a strategic plan to acquire knowledge and intellectual property from researchers, scientists, and the U.S. private sector, the government does not have a comprehensive strategy to combat this threat."[33]

---

[31] GAO, *Export Controls: State and Commerce Should Improve Guidance and Outreach to Address University-Specific Compliance Issues*, (GAO-20-394, May 12, 2020). United States Senate, Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs, *Threats to the U.S. Research Enterprise: China's Talent Recruitment Plans* (November 2019). National Science and Technology Council, *Guidance for Implementing National Security Presidential Memorandum 33 on National Security Strategy for United States Government-Supported Research and Development* (January 2022).

[32] GAO, *Agencies Need to Enhance Policies to Address Foreign Influence* (GAO-21-130, December 2020).

[33] United States Senate, Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs, *Threats to the U.S. Research Enterprise: China's Talent Recruitment Plans* (November 2019), https://bit.ly/31XmAD8 (last accessed January 7, 2022).

Further, in January 2022, the White House's Office of Science and Technology Policy released interagency implementation guidance for strengthening disclosure requirements and facilitating information sharing. For example, as a result of this new guidance, grant and cooperative agreement recipients are required to disclose conflicts of interest, provide biographical sketches, and describe ongoing and pending projects in which they are performing or will perform any part of the work, as well as international collaboration and China affiliations.

Based on this implementation guidance, NASA will finalize its conflict-of-interest policy to require the disclosure of both conflicts of interest and conflicts of commitment.[34] In addition, in contrast to current requirements, the new implementation guidance includes a detailed description of the types of activities that must be disclosed such as organizational affiliations and appointments, participation in programs sponsored by foreign governments, and private equity financing.

[34] A conflict of commitment means a situation in which an individual accepts or incurs conflicting obligations between or among multiple employers or other entities.

CONCLUSION

Insider threats pose a serious risk because of their access to valuable Agency information. In the rapidly evolving cybersecurity landscape, identifying and combating insider threats remains a persistent challenge. Although NASA has taken positive steps to address insider threats to its classified systems by developing mandatory Agency-wide insider threat training, establishing user activity monitoring, and updating the conflict-of-interest policy to combat undue foreign influence, opportunities exist to strengthen the agency's cross-discipline coordination to better understand insider threats for both classified and unclassified systems.

Given its relationship to human behavior, a successful insider threat program looks for anomalies, contextualizes them, and helps facilitate an appropriate response. Acting as a facilitator, the insider threat program assists finding hidden threats and anomalous behavior across users, devices, and applications. As statistics consistently indicate, 85 percent of all insider threat incidents are human related. While Executive Order 13587 was specifically related to protecting classified systems from risks associated with insider threats, NASA should evaluate whether to expand its insider threat program to protect its unclassified critical infrastructure and high-value assets. A robust insider threat program is crucial to matching the cadence of adversaries and balancing the dual tasks of maximizing the utility of partnerships while protecting NASA's intellectual property against theft. At a time when there is growing concern about the continuing threats of foreign influence, taking the proactive step to conduct a risk assessment to evaluate NASA's unclassified systems ensures that gaps cannot be exploited in ways that undermine the Agency's ability to carry out its mission.

RECOMMENDATIONS, MANAGEMENT'S RESPONSE, AND OUR EVALUATION

In order to strengthen NASA's insider threat program, we recommended the Associate Administrator, Assistant Administrator for Protective Services, and the Chief Information Officer:

1. Establish a cross-discipline team to conduct an insider threat risk assessment to evaluate NASA's unclassified systems and determine if the corresponding risk warrants expansion of the insider threat program to include these systems.

2. Improve cross-discipline communication by establishing a Working Group that includes OPS, OCIO, Procurement, human resources officials, and any other relevant Agency offices to collaborate on wide-ranging insider threat related issues for both classified and unclassified systems.

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

Management's comments are reproduced in Appendix D. Technical comments provided by management and revisions to address them have been incorporated as appropriate.

Major contributors to this report include Tekla Colon, Mission Support Director; Scott Riggenbach, Project Manager; Theresa Becker; Joseph Cook; Linda Hargrove; Christopher Reeves; and Matt Ward.

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 MARTIN

Digitally signed by PAUL MARTIN
Date: 2022.03.11 14:40:09 -05'00'

Paul K. Martin
Inspector General

APPENDIX A: SCOPE AND METHODOLOGY

We performed this audit from May 2021 through February 2022 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.

The scope of our audit was NASA's overall risks associated with insider threats. Our audit objective was to determine whether the Agency has established and implemented an effective insider threat program in accordance with federal policies, NASA policies, and best practices. Specifically, we examined whether: (1) NASA's insider threat strategy provides an adequate framework for identifying malicious and unintentional insider threats; (2) NASA implemented appropriate procurement controls to identify and prevent intellectual data theft from foreign adversaries, and (3) NASA developed an adequate set of cybersecurity controls to prevent, detect, and respond to the extraction or manipulation of data and intellectual property.

Methodology

We examined three subject areas: (1) Policies/Directives, (2) Procurement Controls, and (3) Cybersecurity Controls. To gain a holistic view of NASA's Insider Threat program and the broader risk landscape for each subject area, we reviewed numerous federal and Agency policies, regulations, guidance, and industry best practices for managing insider threats. We interviewed responsible NASA officials from the: Counterintelligence division, Security Operations Center, Office of Protective Services Insider Threat Program, Office of Chief Information Officer, Chief Cyber Risk Officer, Senior Agency Information Security Officer, NASA Shared Services Center, and Office of Procurement. Additionally, we met with the NASA OIG Office of Investigations and the National Insider Threat Task Force. Collectively, this informed our understanding of insider threats and helped us assess the effectiveness of NASA's insider threat program.

Key work completed for each subject area is highlighted below.

Policies/Directives. To determine whether NASA's insider threat strategy complied with federal and Agency policies, we reviewed and analyzed policy and framework documents to gain an understanding of insider threats, best practices, and NASA's insider threat program. We interviewed responsible officials to discuss compliance with Executive Order 13587 and progress in identifying malicious and unintentional insider threats. We examined the National Insider Threat Task Force designation of full operating capability to demonstrate NASA's compliance with the mandate. Additionally, we researched ancillary issues such as collaboration and competition in space, foreign government Talent Programs, and NASA insider threat cases.

Procurement Controls. To determine whether NASA implemented appropriate procurement controls to identify and prevent intellectual data theft from foreign adversaries, we reviewed Federal Acquisition Regulations, NASA policy documents, and contract and grant controls. We reviewed historical NASA OIG audit reports for indications that insider threat or cybersecurity considerations were factored into the

awarding of grants or cooperative financial agreements. Additionally, we interviewed responsible officials to discuss contract clause protections against foreign theft of intellectual property.

Cybersecurity Controls. To evaluate whether NASA developed an adequate set of cybersecurity controls to prevent, detect, and respond to the extraction or manipulation of data and intellectual property, we reviewed and analyzed policy and framework documents. We interviewed responsible officials to discuss cybersecurity controls. Additionally, we examined system-related artifacts such as user monitoring and elevated privileges to identify cybersecurity gaps.

Assessment of Data Reliability

We used limited computer-processed data extracted from NASA's IT systems during the course of this audit. Although we did not independently verify the reliability of this information, we compared it with other available supporting documents to determine data consistency and reasonableness. From these efforts, we believe the information we obtained is sufficiently reliable for this report.

Review of Internal Controls

We assessed internal controls and compliance with laws and regulations to determine NASA's overall insider threat risk. Control weaknesses are identified and discussed in this report. Our recommendations, if implemented, will improve those identified weaknesses.

Prior Coverage

In the last 5 years, the NASA Office of Inspector General (OIG) has issued a report of significant relevance to the subject of this audit and GAO has issued reports of interest on this topic. Reports can be accessed at https://oig.nasa.gov/ and https://www.gao.gov/.

- *NASA's Cybersecurity Readiness* (IG-21-019, May 18, 2021)
- *Agencies Need to Enhance Policies to Address Foreign Influence* (GAO-21-130, December 17, 2020)
- *Export Controls: State and Commerce Should Improve Guidance and Outreach to Address University-Specific Compliance Issues* (GAO-20-394, May 12, 2020)
- *TSA Could Strengthen Its Insider Threat Program by Developing a Strategic Plan and Performance Goals* (GAO-20-275, February 10, 2020)

APPENDIX B: INSIDER THREAT MATURITY MODEL

The *Insider Threat Program Maturity Model* provides organizations with a way to benchmark their current ability to monitor, detect, mitigate, and respond to insider threats. The model classifies Insider Threat Programs into the following five categories:

1. *Nonexistent.* The organization has no program or technology in place to detect and respond top insider threats and is unaware of the risk posed by an insider threat.
2. *Reactive.* The organization has no program in place but is aware that insider threats exist. IT is responsible for responding to any realized threat actions.
3. *Proactive.* The organization's focus is on the use of technologies (and the necessary inter-departmental communication to facilitate use) that will help spot any insider threats within a core group of high-risk users.
4. *Predictive.* The organization has a formal program in place that seeks to identify potential or active threats as early on as possible. Program definitions, policies, processes, and technologies are in place organization wide.
5. *Optimized.* The organization's program is holistic, dynamic, and responsive, continually addressing shifting risk and changes in business operations that impact needed policy, process, and technologies.

Maturity levels	Non-existent	Reactive	Proactive	Predictive	Optimized
Goals and objectives	None	Respond to issues as they arise. Investigate as needed to identify what actions took place (if possible).	Monitor users with the highest risk to the organization for inappropriate activity.	Establish appropriate levels of monitoring to all employees. Identify potential threats early. Respond appropriately to both leading and active indicators of threat activity.	Ensure the insider threat program meets the changing needs of the organization through review, adaptation, and optimization of processes, monitoring, and responses.

Maturity levels	Non-existent	Reactive	Proactive	Predictive	Optimized
Awareness	The organization has zero visibility into employee activity, nor into whether they have been or are a victim of an insider threat.	The organization is generally aware of insider threats but are notified by employees or third parties that an act has taken place.	The organization is aware of insider threats and is taking steps to monitor activity in an effort to detect malicious threats by users deemed high-risk to the organization.	The organization is highly aware of insider threats. While the focus is on malicious insiders, the organization is focused on identifying leading indicators of threats in an effort to stop threats before they occur.	The organization has a mature view of insider threat risk —seeing it as something that moves throughout the organization, with every employee as a potential threat. Every source of activity detail is used to provide a full picture of employee risk.
Governance	None	None	Minimally established governance. Informal interaction between Information Technology (IT), Human Resources (HR), and executive teams.	Oversight is established with a formalized team from IT, HR, executive, legal, and security. Threat definitions exist. Basic process and policies are in place.	Insider Threat Program team includes key employees and a designated senior official to head the team. Written policies and processes exist. The team meets using a regular cadence.
Risk assessment	None	None	Identified high-risk individuals and roles requiring monitoring.	Risk levels are defined, high and low-risk roles are assigned. Specific one-off risk assessments occur for individuals.	Risk reviews, reassignment of risk levels and associated monitoring actions occur regularly for both roles and individuals.
Policies	None	None	Either none, or basic policies exist for high-risk individuals, driven by HR or IT.	Policies exist around bring your own devices, proper use of company resources, and maintaining confidentiality.	Policies are routinely examined to ensure they align with other changes in the program.
Monitoring	None	None	Activity is monitored for pre-defined activity thresholds the organization equates as indicators of risk	Activity is monitored for both leading and active indicators of threats based on both static definitions and behavioral analysis.	Activity is monitored for both leading and active indicators of threats based on both static definitions and behavioral analysis.

Maturity levels	Non-existent	Reactive	Proactive	Predictive	Optimized
Processes	None	None	Only informal processes exist around the review of activity and necessary response.	All employees are monitored for leading threat indicators using user behavior analytics and user activity monitoring. Clear and defined processes are in place for high-risk scenarios.	All employees are monitored for leading threat indicators utilizing user behavior analytics and user activity monitoring. Detailed processes are in place for specific low and high-risk scenarios and are routinely evaluated and tested.
Intelligence sources	None	None	Identified high-risk individuals and roles requiring monitoring.	Risk levels are defined, high and low-risk roles are assigned. Specific one-off risk assessments occur for individuals.	Risk reviews, reassignment of risk levels and associated monitoring actions occur regularly for both roles and individuals.
Communications and training	None	None	Basic acceptable use policy in place.	Acceptable use policy in use for all new hires.	Acceptable use policy and security acknowledgement is signed by all employees. Logon banners reaffirm proper usage, confidentiality, and security.

Source: OIG representation of the *2019 Insider Threat Program Maturity Model Report,* https://bit.ly/32ROOQ8 (last accessed January 7, 2022).

A majority of organizations rate themselves as being *proactive* in their approach to insider threats, putting their focus on user behavior—the highest perceived risk to the organization. Activity is monitored using a variety of tools such as log data, user activity and email, with only informal processes in place around response. Likewise, we rated NASA's Insider Threat Program for classified systems as *proactive*.

APPENDIX C: INSIDER THREAT BEHAVIORAL INDICATORS

Rarely does an individual wake up with the intention of betraying their country, compromising national security, or harming their colleagues. Research has consistently shown that malicious acts by insiders are seldom impulsive. That means that something happens over time that contributes to a trusted insider evolving into a malicious one. Usually, it is some sort of perceived life crisis that the individual views as untenable. Eventually, if not addressed in a healthy and adaptive manner, these stressors could influence a person to commit espionage, leak information, engage in targeted violence, or contemplate self-harm.

There are many behavioral indicators of a potential insider threat, too many to list here. According to NASA, the following are some common behavioral indicators:

- Significant changes in personality, behavior, or work habits
- Substance abuse or addictive behaviors (e.g., alcohol or drug abuse, gambling)
- Considerable financial change (e.g., unexplained affluence or excessive debt)
- Seeking access to classified or proprietary information and systems/technology without a "need to know"
- Disregard for security procedures and protocols
- Disgruntled to the point of wanting to retaliate
- Unauthorized removal or unnecessary copy or hoarding of classified or proprietary material
- Access to facilities and/or proprietary information outside of normal work hours

It is important to remember that it may not be a specific indicator in itself, but rather an overall change in behavior. One or several indicators do not inherently make someone an insider threat. However, reporting such concerns or observations to the NASA Insider Threat Program is key so further assessment can be conducted.

Report potential insider threat concerns to:

- NASA Insider Threat Program: hq-insiderthreatprogram@mail.nasa.gov
- The OCIO Security Operations Center: soc@nasa.gov
- Center Protective Services Office
- Your Supervisor
- For imminent threats of workplace violence contact your Center Emergency Response Office

APPENDIX D: MANAGEMENT'S COMMENTS

National Aeronautics and
Space Administration

Mary W. Jackson NASA Headquarters
Washington, DC 20546-0001

March 7, 2022

Reply to Attn of: Office of the Chief Information Officer and Office of Protective Services

TO: Assistant Inspector General for Audits

FROM: Associate Administrator/Assistant Administrator for Protective Services and the Chief Information Officer

SUBJECT: Agency Response to OIG Draft Report, "NASA's Insider Threat Program" (A-21-013-00-MSD)

The National Aeronautics and Space Administration (NASA) appreciates the opportunity to review and comment on the Office of Inspector General (OIG) draft report entitled, "NASA's Insider Threat Program" (A-21-013-00-MSD) dated February 11, 2022.

In the draft report, the OIG makes two recommendations addressed to the Associate Administrator, Assistant Administrator for Protective Services, and the Chief Information Officer.

Specifically, the OIG recommends the following:

Recommendation 1: Establish a cross-discipline team to conduct an insider threat risk assessment to evaluate NASA's unclassified systems and determine if the corresponding risk warrants expansion of the insider threat program to include these systems.

Management's Response: NASA concurs with this recommendation. A cross-disciple team will be assembled to conduct an insider threat risk assessment to evaluate NASA's unclassified systems and determine if the corresponding risk warrants expansion of the NASA insider threat program to include these systems. This team will include but is not limited to representatives from the following organizations:

- Office of Protective Services
  - NASA Insider Threat Program
  - ICAM
  - Cyber Counterintelligence
- Office of the Chief Information Officer
  - Chief Information Security Officer
  - Security Operations Center
  - Deputy CIO, Operations
  - Communications Network Operations Center
  - Workplace & Collaboration
- Inspector General Cyber Crimes Division

The final recommendations of this team will be presented to senior leadership for further consideration.

Estimated Completion Date: December 1, 2023.

Recommendation 2: Improve cross-discipline communication by establishing a Working Group that includes OPS, OCIO, Procurement, human resources officials, and any other relevant Agency offices to collaborate on wide-ranging insider threat related issues for both classified and unclassified systems.

Management's Response: NASA concurs with this recommendation. A Working Group will be established with the above-mentioned parties to collaborate on wide-ranging insider threat related issues for both classified and unclassified systems. The Working Group will conduct an assessment to determine the resources to adequately support program expansion. This assessment will include:

- Working group Concept of Operations
- Defined expanded insider threat scope
- Defined expanded insider threat population
- Resource estimates to support expansion
- Systems to support expansion

The final assessment will be presented to senior leadership for further consideration.

NASA would also like to note that the NASA Insider Threat Program is currently limited to the protection of classified information and clearance holders as required in the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs. The NASA Insider Threat Program is not currently resourced to support any expansion beyond its current scope and duties.

Estimated Completion Date: December 1, 2023.

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 Mark Dodd at (202) 358-1255.

JOSEPH MAHALEY
Digitally signed by JOSEPH MAHALEY
Date: 2022.03.07 14:43:28 -05'00'

Joseph S. Mahaley

JEFFREY SEATON
Digitally signed by JEFFREY SEATON
Date: 2022.03.07 21:16:45 -05'00'

Jeff Seaton

APPENDIX E: REPORT DISTRIBUTION

National Aeronautics and Space Administration

Administrator
Deputy Administrator
Associate Administrator
Chief of Staff
Chief Information Officer
Associate Administrator for Protective Services

Non-NASA Organizations and Individuals

Office of Management and Budget
    Deputy Associate Director, Climate, Energy, Environment and Science Division

Government Accountability Office
    Director, Contracting and National Security Acquisitions
    Director, Information Technology and Cybersecurity Issues

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 and Science

Senate Committee on Homeland Security and Governmental Affairs

House Committee on Appropriations
    Subcommittee on Commerce, Justice, Science, and Related Agencies

House Committee on Oversight and Reform
    Subcommittee on Government Operations

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

(Assignment No. A-21-013-00-MSD)