A Report by a Study Team of the

NATIONAL ACADEMY OF PUBLIC ADMINISTRATION

for the National Aeronautics and Space Administration

Review of the NASA Response to the Academy's Report on Foreign National Access Management

March 2016

National Academy of Public Administration ®

ABOUT THE ACADEMY

The National Academy of Public Administration is an independent, non-profit, and non-partisan organization established in 1967 and chartered by Congress in 1984. It provides expert advice to government leaders in building more effective, efficient, accountable, and transparent organizations. To carry out this mission, the Academy draws on the knowledge and experience of its over 800 Fellows—including former cabinet officers, Members of Congress, governors, mayors, and state legislators, as well as prominent scholars, business executives, and public administrators. The Academy helps public institutions address their most critical governance and management challenges through in-depth studies and analyses, advisory services and technical assistance, congressional testimony, forums and conferences, and online stakeholder engagement. Learn more about the Academy and its work at www.NAPAwash.org.

COVER IMAGES CREDITS

Top left source: https://upload.wikimedia.org/wikipedia/commons/2/2a Space_Shuttle_Atlantis_launches_from_KSC_on_STS-132_side_view.jpg

Top right source: http://www.nasa.gov/centers/stennis/images/content/702983main_SSC-2012-01568.jpg

Bottom left source: http://www.jpl.nasa.gov/news/news.php?feature=4752

Bottom right source: http://i.kinja-img.com/gawker-media/image/upload/s--blMCFJX3--/18dxmd3suvn59jpg.jpg

A Report by a Study Team of the

NATIONAL ACADEMY OF PUBLIC ADMINISTRATION

For the National Aeronautics and Space Administration

March 18, 2016

Review of the NASA Response to the Academy's Report on Foreign National Access Management

STUDY TEAM

Joe Mitchell
Roger Kodat
Susan Adams*
Nicole Camarillo
John Martinez*
Harrison Redoglia
Joe Thompson**
Jonathan Tucker

*Member of the 2014 Study Team

**Project Director of the 2014 Study and Academy Fellow

National Academy of Public Administration
1600 K Street, N.W.
Suite 400
Washington, DC 20006
www.napawash.org

March 2016
Printed in the United States of America
Academy Project Number: 2200

**Academy Fellow*

Foreword

The National Aeronautics and Space Administration (NASA) is an internationally recognized symbol of American ingenuity and success. Since the end of the Cold War, it has built on its Apollo and Space Shuttle program successes by further engaging with citizens of a broader array of countries through the International Space Station and other activities. NASA benefits from global proliferation of technological advancements and cooperation with global partners, but also must take steps to protect itself from any foreign nationals seeking to illegally procure its valuable intellectual and physical assets.

Security incidents involving foreign nationals at NASA's field Centers in recent years led the Agency to engage the National Academy of Public Administration (the Academy) in 2013 to conduct an assessment of its foreign national operations. In 2014, a Panel of Academy Fellows issued 27 in-depth findings and associated recommendations addressing critical components of NASA's foreign national access management. In the past two years, NASA has regularly reported on its progress in further developing this important dimension of its operations.

In February 2016, NASA reengaged the Academy pursuant to a mandate from Congress to review the Agency's progress in implementing the 2014 Panel recommendations. This review by an Academy study team evaluates the extent to which NASA has mobilized and integrated its resources to institutionalize a world-class program to manage foreign national access in order to safeguard its physical and intellectual assets. The results are intended to contribute to NASA's on-going efforts to maintain its trajectory towards on-going improvements in its foreign national access management program.

As a Congressionally chartered non-partisan and non-profit organization with over 800 distinguished Fellows, the Academy brings seasoned experts together to help government organizations address their most critical challenges. The Academy has long had a special connection with NASA given that one of our principal founders, James Webb, was the Agency's second Administrator. I wish to express appreciation to NASA for assisting the Academy study team during this review, and to three distinguished Academy Fellows who provided expert guidance to the project study team.

Dan Blair
President and Chief Executive Officer
National Academy of Public Administration

Table of Contents

Acronyms

ACP	Access Control Plan
BSA	Baseline Services Assessment
BSSC	Business Service Steering Committee
CCS	Center Chief of Security
CCPS	Center Chief of Protective Services
CDM	Continuous Diagnostics and Monitoring
CEA	Center Export Administrator
CI	Counterintelligence
CI/CT	Counterintelligence/Counterterrorism
CISA	Counterintelligence Special Agent
CISO	Chief Information Security Officer
CNOS	Consolidated Network Operations Services
DHS	Department of Homeland Security
DOD	Department of Defense
DSS	Defense Security Service
EBPro	External Border Protection
EC	Export Control
EIB-NAC	Enterprise Internal Border-Network Access Control
FITARA	Federal Information Technology Acquisition Reform Act
FNAM	Foreign National Access Management
FSO	Facility Security Officer
FY	Fiscal Year
HQ	Headquarters
IdMAX	Identity Management and Account Exchange
IFR	Integrated Functional Review
IIR	Intelligence Information Reports
ISFR	Integrated Security Functional Review
ITAR	International Traffic in Arms Regulations
IVC	International Visit Coordinator
LPR	Lawful Permanent Resident
MBT	Mission Backbone Transition
NAII	NASA Advisory Implementing Instruction
NAMS	NASA Access Management System
NASA	National Aeronautics and Space Administration
NEACC	NASA Enterprise Applications Competency Center
NIST	National Institute of Standards and Technology
NOC	Network Operations Center

NPD	NASA Policy Directive
NPR	NASA Procedural Requirement
OCIO	Office of the Chief Information Officer
OIG	Office of the Inspector General
OIIR	Office of International and Interagency Relations
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OPS	Office of Protective Services
PIV	Personal Identity Verification
SATERN	System for Administration, Training, and Educational Resources for NASA
SME	Subject Matter Expert
SOC	Security Operations Center
TTCP	Technology Transfer Control Plan

Executive Summary

The National Aeronautics and Space Administration (NASA) is perhaps the most internationally recognized symbol of American ingenuity. Decades of diligent research and development by NASA employees and contractors have yielded enormously valuable physical and intellectual assets. An important element in NASA's success is the many and innovative ways the Agency collaborates with American industry and international partners, both large and small, to achieve its mission. NASA's obligation toward asset protection on one hand, and fostering a collaborative operating culture engaging with domestic and foreign partners on the other hand, requires promulgation of thoughtful, balanced policies and procedures that help achieve both of these critical objectives as effectively as possible.

Given the importance of these issues, NASA contracted with the Academy in 2013 to conduct a review of its Foreign National Access Management program (FNAM). In 2014, the Academy formed a Panel chaired by former Attorney General Dick Thornburgh that issued a sensitive but unclassified report entitled "An Independent Review of Foreign National Access Management" (2014 Panel Report) that presented 27 detailed findings and associated recommendations based on the work of a Panel of Academy Fellows. The purpose of this follow-up review is to evaluate whether NASA has taken the necessary actions to address the 2014 Panel Report's recommendations at headquarters and in Centers.

The Academy study team found that NASA has taken actions to address each of the 27 recommendations found in the 2014 Panel Report, as evidenced by demonstrable progress made during the last 26 months. While the status of completion across the wide range of recommendations varies, none were ignored. The Agency clearly embraced the importance of the 2014 Panel Report and followed the Panel's risk-based prioritization of recommendations to guide specific investment of substantial resources to develop the Foreign National Access Management (FNAM) Program.[1] It is clear from discussions with and documentation from both Centers and Headquarters that FNAM has improved significantly during the past few years. Furthermore, NASA is committed to further enhance this program through periodic, rigorous review and improvement in the future.

NASA has not, however, fully implemented a number of key recommendations, including promulgation of the FNAM Operations Manual. Although the Agency has made important progress to these additional areas, the Academy study team was not able to completely assess their impact on the FNAM Program at this time. Still, the Academy study team deems that NASA is on a path toward institutionalizing an integrated FNAM Program that readily incorporates the activities of its components into daily Center operations, and can thus remain a priority for future NASA senior leaders. As part of this review, the study team identified additional work that NASA should do to further develop the FNAM program.

[1] Establishment of the FNAM Program is a cooperative effort requiring coordination between the Office of Protective Services, the Office of the Chief Information Officer, and the Office of International and Interagency Relations, in consultation with NASA Centers.

Section 1: Introduction

Section 1.1: Summary

The mission of the National Aeronautics and Space Administration (NASA) is to "pioneer the future in space exploration, scientific discovery and aeronautics research." To be successful, NASA (sometimes referred to in this report as the Agency) must work collaboratively with individuals from many nations on a variety of innovative scientific and engineering projects. Given the high value of NASA's intellectual and physical property, it is incumbent upon its employees and contractors to take prudent steps to protect valuable assets while also supporting NASA's vital international work. An integrated set of practical policies and procedures connected with protective services, information technology, and international relations are necessary to address this important dimension of NASA's operations.

In 2013, NASA contracted with the National Academy of Public Administration (the Academy) to conduct a review of its foreign national operations. In 2014, the Academy issued a report (hereafter referred to as the 2014 Panel Report[2]) entitled "An Independent Review of Foreign National Access Management"[3] that presented 27 detailed findings and associated recommendations (see Appendix C) based on the work of a Panel of Fellows chaired by Dick Thornburgh, a former Attorney General of the United States. The recommendations are summarized in the 2014 Panel Report's Executive Summary (see Appendix D):

- Manage Foreign National Access Management (FNAM) as a program;
- Reduce flexibility given to Centers to interpret FNAM requirements;
- Determine critical assets and build mechanisms to protect them;
- Correct longstanding IT security issues;
- Change several aspects of NASA culture; and
- Communicate the importance of these changes clearly, firmly, and consistently.

The Fiscal Year (FY) 2015 Commerce, Justice, and Science appropriations report mandated NASA to reengage the Academy to formally review NASA's progress in implementing these corrective actions. The depth of the Academy study team's[4] assessment was limited by NASA's requirement that this review be completed during a 7-week timeframe.

Section 1.2: Scope

The scope of this follow-up assessment encompasses five distinct components of the FNAM Program:

1. Foreign national identity management;
2. Hosting and escort procedures;
3. Export controls;

[2] This report was an official report of an Academy Panel.
[3] Due to the sensitive nature of several topics addressed in the Panel's report dated January 2014, NASA deemed it to be sensitive but unclassified, and thus the full 2014 Academy Report was not made available to the public.
[4] The Academy study team received counsel from an Expert Advisory Group of three Academy Fellows. Short biographical information about these individuals is provided in Appendix A.

4. Counterintelligence; and
5. Information technology security.

For each component, this follow-up review offers an assessment as to whether:

1. NASA has taken the necessary actions to address the recommendations from the 2014 Panel Report and assess any risks that may be associated with shortcomings with respect to any of these recommendations;
2. These actions have been communicated to and/or implemented at the ten NASA field Centers (Centers); and
3. There are additional considerations to assist NASA in moving forward with a highly reliable FNAM Program.

In assessing progress, we realize that actions connected with some recommendations may take several years to design, develop, and fully implement. We note NASA's commitment to regularly review and update policies and procedures connected with FNAM Program. As such, this review of NASA's progress should be supplemented by a periodic program re-assessment as the program matures.

Section 1.3: Methodology

The Academy study team reviewed NASA's quarterly FNAM progress report updates submitted to Congress[5] and held discussions with both Agency senior leadership and Center[6] representatives (see Appendix B for a list of interviewees). Our meetings were generally divided into three major categories: Agency Headquarters (HQ) staff; FNAM component leaders[7] working in five Centers,[8] and project-focused employees in several of the five Centers as an attempt to validate whatever progress was described during the HQ and component leader meetings.

Specifically, the study team:

- Received briefings from NASA Agency executives responsible for each component;
- Engaged in FNAM component-specific focus groups via conference call with representatives from each of the five NASA Centers visited during the course of the 2014 Panel Report;[9]
- Met with senior leaders to discuss overall progress on the recommendations; and
- Reviewed updated FNAM-related manuals, training modules, and access management control systems.

[5] NASA's congressional updates are deemed Sensitive But Unclassified; they are not available to the public.
[6] There are 9 NASA Centers and one Federal Funded Research and Development Center, Jet Propulsion Laboratory, located around the country.
[7] We met with CI and export control agents, as well as the Office of the Chief Information Officer and Chiefs of Security from most of the five Centers.
[8] CI meetings were convened with 9 Centers and one Federally Funded Research and Development Center, Jet Propulsion Laboratory.
[9] Goddard Space Flight Center, the George C. Marshall Space Flight Center, the Langley Research Center, the Ames Research Center, and the Jet Propulsion Laboratory.

Section 1.4: Summary of Findings

Overall, NASA has taken actions to address each of the 27 recommendations found in the 2014 Panel Report as evidenced by demonstrable progress made during the last 26 months. While the status of completion across the wide range of recommendations varies, none were ignored. The Agency clearly embraced the importance of the 2014 Panel Report and followed the Panel's risk-based prioritization of recommendations[10] to guide specific investment of substantial resources to develop the FNAM Program.[11] It is clear from discussions and documentation from both Centers and HQ that FNAM has improved significantly during the past few years. Furthermore, NASA is committed to further enhance this program through periodic, rigorous review and improvement in the future. Yet it is important to note that NASA has not fully implemented a number of key recommendations, including promulgation of the FNAM Operations Manual. Although the Agency has made important progress to these additional areas, the Academy was not able to completely assess their impact on the FNAM Program at this time. That said, we deem that NASA is on a path toward institutionalizing an integrated FNAM Program that readily incorporates the activities of its components into daily Center operations, and can thus remain a priority for future NASA senior leaders. This review also articulates additional work to be done.

Section 1.5 Review Structure

This review contains five sections in all; the following four sections cover the FNAM Program and its components: FNAM Program development, including foreign national identity management and hosting and escorting procedures; export controls; CI; and information technology security. Each section contains a broad summary assessment of NASA's progress in that area; an assessment of individual recommendations; and may also contain additional considerations.

[10] The Risk Map was presented in Figure 4.3 in the 2014 Academy Report and is shown in Appendix F. Many of the higher risk recommendations have been addressed already; some are still being implemented, as is noted in this review.

[11] Establishment of the FNAM Program is a cooperative effort requiring coordination between the Office of Protective Services (OPS), the Office of the Chief Information Officer (OCIO), and the Office of International and Interagency Relations (OIIR), in consultation with Centers.

Section 2: Foreign National Access Management Program

Section 2.1: Summary

Overall, NASA has made significant progress in establishing an FNAM Program. Because some significant aspects of the FNAM Program have been developed but not yet implemented (for example, an operations manual and training modules), the study team was only able to evaluate NASA's progress on the development of these efforts. NASA has plans to assess the effectiveness of these changes once they have been put into practice at the Centers. Generally, we deem NASA's current efforts underway to be promising and should provide the necessary tools for standardizing compliance with policies and procedures across Centers. Furthermore, the study team observed a general increased awareness of FNAM issues and requirements at Centers resulting from multiple outreach efforts by HQ.

Section 2.2: Assessment

Eighteen of the 27 recommendations issued in the 2014 Panel Report fall under two main objectives: (1) managing FNAM as a program and (2) reducing the flexibility given to Centers to interpret FNAM requirements. In achieving these objectives, HQ was able to address multiple recommendations with a single action. Accordingly, this section will be organized by these two objectives, with a notation of the applicable recommendations.

Managing FNAM as a Program (*2014 Academy Report Recommendations 14, 21, 24b, 26, 27)*

In the 2014 Panel Report, the Panel emphasized the need to manage foreign national access under a structured program, especially given NASA's highly decentralized organizational structure and independent Centers. In response, NASA created a management structure for the program and began developing specific components including updated policies, an operations manual, program website, new and enhanced training modules, and an enhanced integrated functional review process.

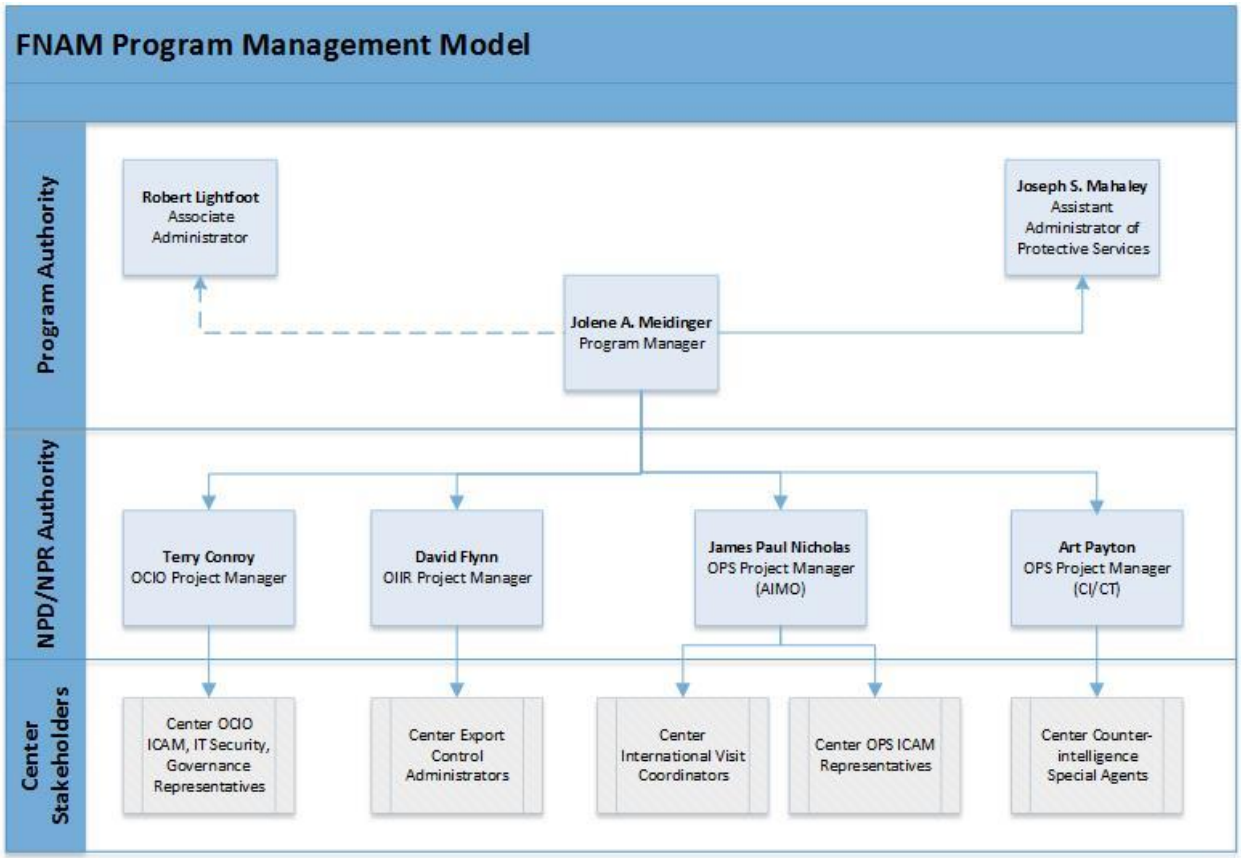
> FNAM Program Management Structure (2014 Academy Panel Recommendation 21, 24(b)[12]) **Recommendation 21 was implemented and NASA implemented a solution that addresses the intent of Recommendation 24(b).**
>
> As recommended in the 2014 Panel Report, the FNAM Program is overseen by a program manager from the Office of Protective Services (OPS) who reports to both the NASA Associate Administrator and the Assistant Administrator for OPS. The program manager serves as the initial Agency point of contact for all FNAM-related issues and leads the coordinated effort among OPS, the Office of the Chief Information Officer (OCIO), and the Office of International and Interagency Relations (OIIR) in achieving program objectives.[13] Each office has a project manager who reports directly to the FNAM Program manager. OPS designated two project managers, one who is responsible for foreign national identity management and hosting and escort procedures and a second project manager

[12] Recommendation 24(a) is addressed in Section 4 of this report and 24(c) is addressed in Section 3.
[13] NASA, "FNAM Program Commitment Agreement," June 2014.

who is responsible for counterintelligence. OIIR has a designated project manager responsible for export controls and OCIO has a designated project manager responsible for information technology security (see Diagram 2.1). The Panel also recommended that OPS be elevated onto a level with more direct reporting responsibilities to the Office of the Administrator to ensure that FNAM issues receive the appropriate amount of leadership attention. NASA agreed to evaluate the reporting relationships of OPS to ensure there are no unintended constraints on communications and critical reporting requirements and there is now a "dotted line" relationship between OPS and Agency leadership. As discussed in the subsequent sub-section on NASA's outreach and awareness efforts, both the NASA Administrator and Associate Administrator have been engaged in communicating with personnel on the importance of adhering to FNAM requirements.

The study team observed a strong working relationship among the program manager for FNAM and respective project managers from each related office. It was evident that HQ approached developing the program with an integrated team representing all components of FNAM.

Diagram 2.1



Outreach and Awareness Efforts (2014 Academy Panel Report Recommendations 14, 26, 27): **These recommendations have been implemented.**

In the 2014 Panel Report, the Panel recommended that NASA Agency leadership and Center Directors periodically and formally reiterate to all employees and contractors the importance of Security and CI/CT Programs and functions and each individual's responsibility to support them. NASA responded by engaging in stakeholder outreach to increase awareness of FNAM requirements. Following the release of the 2014 Panel Report, the NASA Administrator and Associate Administrator addressed the importance of compliance by all personnel with the FNAM process. The Assistant Administrator for Protective Services also began delivering a monthly address to NASA employees on various security issues related to FNAM. The first such presentation focused on procedures and policies for coordinating visits from foreign nationals. The Assistant Administrator informed the study team that Center leaders have submitted requests for copies of these presentations. When asked about awareness efforts on FNAM issues by HQ, some interviewees mentioned these presentations by the Assistant Administrator. HQ also conducted town hall meetings at individual Centers for program and project managers that were focused on FNAM issues.

The 2014 Panel Report also recommended that NASA engage all stakeholders in the identification of best practices. In fact, the Panel highlighted the fact that some Centers had developed and published their own FNAM procedural requirements that were found to be more practical and user-friendly. In an effort to implement an Agency-wide set of operating standards**,** NASA engaged stakeholders in developing the FNAM Program, including improvements to existing processes and procedures.

When NASA began the process of developing the FNAM Program, the FNAM Program Manager presented at Agency-hosted conferences for Center stakeholders, sharing findings from the 2014 Panel Report as well as the proposed program model and plan. HQ also began roundtable FNAM discussions designed to bring together Center stakeholders and subject matter experts (SMEs) in addition to regularly occurring meetings with groups responsible for different areas related to foreign national access management. Agency staff met most frequently with Center Chiefs of Security and International Visit Coordinators (IVCs) and continues to do so on a monthly basis (see Appendix E).

During study team interviews with stakeholders at multiple Centers, participants confirmed HQ outreach efforts and opportunities to participate in the process of developing program requirements and procedures. That said, several interviewees noted that the turn-around time to provide feedback was too short and did not allow participants to provide thorough feedback; and some stakeholders noted that more SMEs involved in processing foreign nationals at the Centers should be included in this process. Overall, interviewees across Centers recognized HQ efforts to improve the FNAM process and many stated that they were a step in the right direction.

The 2014 Panel Report identified NASA culture as an impediment to sharing best practices and improving FNAM capabilities, in part due to a sense of competition among Centers. HQ efforts over the past two years to engage stakeholder groups representing multiple Centers in developing the

FNAM Program have helped to change the culture to one of more sharing and cooperation in this area. For example, study team interviews with participants in stakeholder groups revealed that Centers were able to share their concerns with one another and identify areas where many were struggling with similar issues as well as sharing best practices. In fact, the study team encourages HQ to formalize this process of sharing best practices across Centers.

Reducing the Flexibility given to Centers to Interpret FNAM Requirements *(2014 Academy Report Recommendations 1, 2, 3, 4, 5, 14, 15, 16, 17, 22, 25, 27)*

The 2014 Panel Report emphasized that NASA needed to provide consistent guidance, training, and oversight across the Agency. The Panel acknowledged that NASA Procedural Requirements (NPRs) and Policy Directives (NPDs) pertaining to FNAM were "comprehensive, well-written, and easily accessible." However, the Panel's 2014 Panel Report stated that they did not adequately "provide effective and practical guidance on *how* those responsible individuals, officials, and entities were to perform the designated tasks." The 2014 Panel Report noted that NPRs and NPDs were infrequently utilized in the performance of day-to-day tasks and assignments; most personnel relied on their own experience or that of their peers when faced with an issue or problem.

Consistent with the recommendations from the 2014 Panel Report, NASA addressed these issues, including developing both interim policy guidance and creating the FNAM Operations Manual and website to provide standardized and centralized guidance for all Centers. Training modules are also being developed to strengthen compliance with policies and procedures related to FNAM. Enhancements to NASA's Identity Management and Account Exchange (IdMAX) system will further strengthen compliance with FNAM requirements and improve oversight of foreign national access across the Agency.

Interim Policy Guidance (2014 Academy Panel Recommendation 5): **This recommendation has been implemented.**

NPR 1600.4 contains all of the requirements for FNAM. In 2014, after review of the 2014 Academy Report's recommendations, OPS issued interim policy guidance to provide further clarification on foreign national identity management and escorting requirements.[14] The interim guidance also addressed the 2014 Panel Report's recommendation that Agency staff develop procedures and protocols for Centers to follow when a positive "hit" is obtained in a Visual Compliance[15] check. This guidance has been incorporated into an update to NPR 1600.4 that aligns with the policies and procedures featured in the new FNAM Operations Manual discussed below. The updated policy and operations manual are both awaiting approval by HQ prior to being released to NASA personnel.

FNAM Operations Manual (2014 Academy Panel Recommendations 1, 2, 3, 16): **These recommendations have been developed but are awaiting approval prior to being implemented.**

[14] NASA, "Interim Policy Regarding Foreign National Access Management," April 2, 2014.
[15] The Visual Compliance check provides a method to determine if a foreign national has been identified as a person of interest on any list maintained by a restricted party screening authority.

At the time of the 2014 Panel Report, NASA employees had to seek procedural information with respect to FNAM components in various locations and it was not always clear whom to go to when issues arose. While NASA developed the FNAM Operations Manual as recommended by the Panel, it is important to stress that it cannot be implemented in the Centers until it receives final approval from HQ, which is expected soon.

The study team deems that the Operations Manual provides critical information on processes and information that all Centers are expected to follow and serves as a comprehensive resource for those engaged in FNAM. The materials offer a clear overview of processes and procedures, and the proper channels to follow for support. Furthermore, it contains "helpful tip" sidebars and includes references indicating when a specific topic area is also discussed in other sections. The online version of the Operations Manual will include embedded hyperlinks for additional information as well as checklists and flowcharts that can be printed and used as job aids. The study team recommends that NASA move as expeditiously as possible in providing the new manual to the Centers.

FNAM Website (2014 Academy Panel Recommendation 14): **This recommendation has been implemented.**

NASA developed the FNAM website, launched in 2015, to increase awareness of this program and to provide practical information and resources for NASA employees and contractors; it is located on the OPS home page. While the study team believes this to be an important achievement responding to the 2014 Panel Report, further actions could be taken to enhance its use. For example, several individuals interviewed by the study team were either unaware of the website or were relying on other resources to find information. One interviewee noted that many questions were not addressed on the website. Therefore, continued focus on communicating the website's value should be a priority.

Training Modules (2014 Academy Panel Recommendation 15): **This recommendation contains components that are developed and implemented, and others that are in the process of being developed.**

Another critical aspect of the FNAM Program is standardizing the training that employees receive to ensure that policies and procedures related to FNAM are streamlined and consistently implemented across Centers. In the 2014 Academy Report, the Panel observed that approving foreign nationals for access to NASA facilities and systems varied significantly from Center to Center. Study team interviews revealed that this continues to be the case with respect to Centers following varied practices and procedures. To address this issue, NASA is in the process of developing the following training modules:

1. *NASA Foreign National Escort Training*

   NASA plans to upload the foreign national escort training to the Agency's online training platform, System for Administration, Training, and Educational Resources for NASA (SATERN) by April 2016. Not all Centers host visits by foreign nationals and some Centers are subject to additional access requirements because of their physical location. For

example, the Marshall Space Flight Center is located on property under the U.S. Department of Defense's (DoD) jurisdiction and must follow both NASA and DoD regulations for hosting foreign nationals. Therefore, based on feedback from Center stakeholders, Center Chiefs of Security and IVCs, Center specific information slides will be incorporated into the foreign national escort training module.[16]

2. *Enhanced Personal Identity Verification (PIV) Requestor and PIV Sponsor Training*

   The FNAM Program plans to update the PIV requestor and sponsor training currently available on SATERN and is in the process of reviewing the module to assure it aligns with current policy and regulations. A general education of the FNAM Program will also be incorporated into this training module which is expected to be released in September 2016.

3. *International Visit Coordinator Training*

   The FNAM Program has provided target training to IVCs (e.g. visas/passports) through monthly/quarterly IVC teleconferences. Recognizing a need for additional training on the proper processes and procedures executed in the IVC role, NASA plans to develop a new training module that will be uploaded to SATERN. NASA estimates that the training will be available in December 2016.

Integrated Security Functional Reviews (2014 Academy Panel Recommendations 17, 22, 23): **NASA implemented actions that respond to the intent of these recommendations.**

Three recommendations from the 2014 Panel Report call for establishing enhanced compliance and accountability mechanisms within the agency's existing Integrated Functional Reviews (IFRs):

- NASA should expand periodic IFR and CI/CT Program Reviews conducted at Centers to evaluate the procedural components comprising the FNAM Process so that they also measure effectiveness and efficiency. (Recommendation 17)
- NASA should create an Independent Review Team led by OPS that included OCIO, OIIR and Center representatives to biennially review all Centers to ensure FNAM policy requirements are being met. (Recommendation 22)
- NASA should create an Asset Protection Oversight Board to oversee safety and security of NASA assets in the field. (Recommendation 23)

Rather than developing an independent review team, NASA leveraged OPS's existing functional review by incorporating it with the annual reviews conducted by OIIR, OCIO, and CI/CT. This collaboration represents the integrated security functional review NASA now conducts at each Center. Developing this review process included creating FNAM-specific questions in 2015, following roundtable discussions with Centers. NASA began conducting reviews with the new FNAM-focused questions in 2015 in addition to including a representative from the FNAM Program

[16] NASA document provided to the study team, March 2016.

on review teams. FNA-targeted questions were finalized based on lessons learned from reviews at the first three Centers. Additional questions will be added once the updated policy and Operations Manual have been promulgated. As the Agency continues to enhance this process, NASA should ensure that these reviews result in comprehensive assessments of each Center's implementation of FNAM Program requirements.

NASA agreed with the intent of the Panel's recommendation to create an Asset Protection Oversight Board, but chose to leverage the Agency's existing boards that perform various aspects of oversight for the safety and security of NASA assets in the field. The study team recommends that, when performing oversight responsibilities, the existing council should keep in mind the intent of the Panel's original recommendation: "to protect all of NASA's valuable ITAR and EAR technical data and proprietary information, not simply the data potentially exposed to foreign nationals." This includes compiling threat assessments from security, CI/CT, and the Chief Information Security Officers (CISOs) into comprehensive Center and Agency threat/risk assessments.

Identity Management and Account Exchange (IdMAX) System Enhancements (2014 Academy Report Recommendations 4, 16): **Recommendation 4 is in the process of being implemented. Recommendation 16 is in development and has not yet been implemented.**

IdMAX is an automated system designed to capture and store data needed to confirm the identity of individuals and determine their level of access to NASA facilities and systems for which they are authorized. The Panel recommended that NASA incorporate FNAM requirements into IdMAX including the capability to create a Technology Transfer Control Plan (now referred to as an Access Control Plan or ACP) for individuals that allows the Agency to automatically limit access to NASA facilities and systems based on specific criteria. The Panel also recommended that NASA simplify and streamline IdMAX workflows and business processes to address the vulnerability resulting from NASA personnel who might wish to circumvent security procedures seen as too cumbersome.

Some enhancements to IdMAX, such as making ACPs accessible within IdMAX, have been implemented, but most are still under development. However, NASA is addressing the highest risk first through enhancements related to managing access by longer-term, worker-level, foreign nationals. These enhancements are scheduled for completion in the summer of 2016. The streamlining of business processes for short-term (<30 days) visitors is scheduled to take place following completion of the higher priority enhancements.

While implementation is still underway, it is clear that NASA has embraced this recommendation. NASA reprioritized funding and personnel to incorporate recommended enhancements into its ongoing IdMAX modernization project. It is on track to implement these enhancements ahead of the originally scheduled deadline for completing the original modernization project.

The 2014 Panel Report also found that not enough stakeholders and end users were involved in discussions for improving the IdMAX system. In response, NASA developed a process that engaged these groups in planning and testing new IdMAX applications. Study team interviews revealed that NASA is making a good faith effort to engage stakeholders and user groups. However, some participants stated that their input was not sought until late in the development process and that

more time was needed for user testing. Based on this feedback, the IdMAX development group plans to engage stakeholders and end-users earlier in the process and allow more time for testing the next round of IdMAX enhancements.

Also, in keeping with leading practice, NASA is using an agile approach to developing IdMAX enhancements, which includes the modular development of capabilities together with regular, ongoing engagement of stakeholders and end users in planning and testing as described above. This should mitigate the risk of delays and budget overruns commonly associated with traditional development approaches.

Section 2.3 Additional Considerations

Based on feedback received from NASA Center personnel involved in FNAM, the study team recommends that NASA consider taking the following actions to enhance the FNAM Program's current development efforts:

- **Raise awareness of the existence of an FNAM Program and its components.** NASA should develop a communication plan to ensure Agency-wide awareness of the concept of FNAM as a program and its accompanying resources (e.g., Operations Manual, website). This approach would reinforce buy-in of the standardized approach the program seeks to achieve, moving Centers away from the independent model they have become accustomed to rely on. Once the Operations Manual becomes available to employees, NASA should consider providing workshops at Centers, acquainting employees with its contents and online features to ensure that this resource is being utilized.

- **Establish communities of practice to share best practices and lessons learned.** NASA should create a formal community of practice among the Centers so that they can share practices and procedures they have developed to meet FNAM Program objectives.

- **Develop a formal process for users to submit feedback.** NASA should develop a formal process for individuals to submit recommendations for improvements to newly developed resources such as the Operations Manual and training modules. Developing such a process will allow HQ to get more timely input on program improvements and respond more readily to stakeholder concerns.

Section 3: Export Controls

Section 3.1: Summary

Export Control (EC) activities were addressed in recommendations 19, 20 and 24c in the 2014 Panel Report. Based on the interviews that have been conducted with personnel from HQ and five Centers, as well as reviews of NASA's EC Operations Manual, it is clear that the EC Program has been enhanced to the degree that overall agency EC awareness has improved. The EC Program inconsistencies observed during the 2014 study have been reduced or eliminated; all recommendations have been implemented.

Section 3.2: Assessment

Recommendation 19 *urges NASA to (a) provide a detailed EC manual to serve as a standardized guide to Center employees, (b) issue a strongly worded communication from senior management to NASA employees that affirms the agency's commitment to export compliance, (c) conduct outside periodic reviews of each Center's EC activities, and (d) require HQ to endorse any CEA field job is filled, as well as allow HQ to provide input into each field CEA annual rating.* ***This recommendation has been implemented.***

NASA's revised EC Manual is prefaced with a message from NASA's Administrator that stresses the importance of the EC Program and the responsibility of everyone at NASA to use the program to safeguard the technologies that are crucial to NASA's mission. NASA's revised EC manual contains an easy-to-use interactive index that contains topics that would be of value to both EC customers and the Center Export Administrators (CEAs) who provide the appropriate guidance for sharing protected technical data.

Agency-wide EC awareness is a crucial component of any successful export compliance program. NASA has taken the important step of having EC awareness promoted by its senior executive management team. NASA's Administrator and many of its senior executives have been promoting the importance of EC compliance to all NASA employees through the use of letters, internal electronic messaging and personal discussions at Center town hall meetings. During recent interviews conducted by the Academy study team it was noted that NASA employees have a much better understanding of EC regulations as a result of NASA's outreach program. This greater EC awareness will, in turn, afford greater protection to NASA's sensitive protected technologies. A Center staff employee noted that within a year of the issuance of the 2014 Panel Report, there was a greater emphasis placed on the proper labeling of International Traffic in Arms Regulations (ITAR)-restricted documents to ensure that they are safeguarded on internal IT systems in order to avoid unauthorized dissemination. Greater EC awareness was posited as the main reason for this improvement regarding technical data protection and security.

In addition to enhancing EC training through a multi-tiered approach, and raising the level of EC awareness through enhanced training, NASA has also taken appropriate steps to ensure that its EC community works closely with other programmatic components that contribute to the FNAM Program. Improved EC compliance through enhanced training has yielded stronger collaboration between FNAM Program components.

The 2014 Panel Report's recommendation for regular outside periodic reviews of each Center's EC Program has been addressed by including CEAs on functional review teams that conduct ongoing/recurring reviews of each Center's security, EC, and IT protection programs. These teams are comprised of reviewers from the separate functional disciplines as well as from other Centers in an effort to enhance the objectivity of the reviews. The Academy study team considers this initiative to be an important step in NASA's effort to create an FNAM Program that receives the support of all of the cross-functional organizational areas involved in foreign national access.

In addition, based on the direction of NASA's Associate Administrator in 2014, OIIR is now included in the selection of new CEAs, as well as having input into their annual performance appraisals. The 2014 Panel Report suggested this action would strengthen the linkage between Center CEAs and their HQ counterparts.

Recommendation 20 *states that NASA should revisit its current export training program and develop an improved and more effective standardized training program for educating both specialized Center export control personnel as well as other NASA employees who need to understand US export regulations.* ***This recommendation has been implemented.***

The issue regarding inadequate and inconsistent EC training has been addressed through creation of a multi-tiered EC training program designed to meet the needs of Center EC specialists as well as Center staff employees who need a less technical level of EC awareness. The study team contends that the enhanced training and the heightened level of overall EC awareness has improved NASA's ability to protect valuable sensitive technological data and reduced data vulnerabilities. One important note to emphasize is that making EC training mandatory would help to further improve NASA's return on this investment towards continued cultural awareness and EC compliance throughout the agency.

In addition to creating a well-designed EC Operations Manual, enhancing EC training through a multi-tiered approach, and raising the level of EC awareness, NASA has also taken appropriate steps to ensure that its EC community works closely with the other programmatic components that contribute to the FNAM Program. During HQ briefings and interviews the Academy review team was advised that NASA's newly created FNAM Program was developed through the collaborative efforts of OIIR and OPS and the OCIO. In addition, it appears that at the Centers the team approach towards FNAM is also improving. CEAs were cited by Center staff employees for their prompt attention to requests for assistance from the Center program staff employees that they serve.

Recommendation 24c *calls for developing strong organizational relationships between certain key FNAM-related jobs in the field, specifically CEA and Counterintelligence Special Agents (CISAs) with their HQ counterparts.* ***This recommendation has been implemented.***

This recommendation has been addressed by including CEAs on functional review teams that conduct ongoing/recurring reviews of each Center's security, EC, and IT protection programs. These teams are comprised of reviewers from the separate functional disciplines as well as from other Centers in an

effort to enhance the objectivity of the reviews. The study team considers this initiative to be an important step in NASA's effort to create a FNAM Program that receives the support of all of the cross-functional organizational areas that are involved in foreign national access. Also, the study team has learned that NASA's newly created FNAM Program was developed through the collaborative efforts of the OIIR and OPS and the OCIO. In addition, it appears that at the Centers the team approach towards FNAM is also improving.

The study team believes that NASA has taken several important steps towards improving and insuring that the EC Program receives the support that is necessary to protect NASA's sensitive technical data from unauthorized dissemination. With the inclusion of EC in the cross-functional approach taken to develop the FNAM Program it should serve to help ensure the future success of the new FNAM Program.

In sum, the study team is very encouraged by the following efforts NASA has taken to improve its EC Program: increased agency cultural awareness; an improved EC operations manual; enhanced training; a partnership between Agency and Center management in the selection and retention processes for Center EC staff; and EC participation in cross functional Center reviews. The study team believes that the overall FNAM Program has benefited as a result of NASA's improved EC Program.

Section 3.3: Additional Consideration

Based on feedback received from NASA Center personnel involved in EC, the study team recommends that NASA consider taking the following actions to enhance EC's current development efforts:

- **Center senior managers should be more vigilant where their EC resources are concerned.** Of concern to some of the CEAs is the fact that, as the level of EC awareness grows at the Centers, the current staffing levels at some Centers might not be sufficient to handle an increase in the EC workload. The improvement in NASA's EC Program may require that Center senior management add additional resources to their EC staffs in order handle the increase in EC workload that usually accompanies improved awareness and increased compliance.

Section 4: Counterintelligence

Section 4.1: Summary

NASA agreed with the implementation of five of the six counterintelligence (CI) recommendations of the 2014 Panel Report. Although NASA leadership decided not to implement one recommendation, NASA has taken actions that demonstrate it agreed with its intent. Most of the recommendations have been fully implemented and others are ongoing. Two of the changes went above and beyond the 2014 Panel Report's recommendations.

Section 4.2: Assessment

Recommendation 9: *NASA should increase the number of CI personnel to adequately handle the threat from foreign nationals and to coordinate the creation, procurement, and distribution of effective CI training resources.* ***This recommendation has been implemented.***

NASA now has a fully staffed Counterintelligence/Counterterrorism (CI/CT) Division,[17] including a Director at the SES level and two GS-15 Regional Directors. Each Center currently has a GS-14 Lead Counterintelligence Special Agent (CISA) as well as a second CISA. Two Cyber CI professionals have also been added, raising the complement of the full time CI/CT staff from 19 to 26. These changes went beyond the 2014 Academy Panel recommendations by promoting the top three CI agents into commensurate positions with their partners in the US Intelligence Community.

This attention given to the NASA CI Program was further evident at the 2015 annual CISA conference, attended by National Counterintelligence Executives, the FBI Agent in charge of Counterintelligence, the NASA Administrator, the Assistant Administrator, Office of Protective Services, and the host Center Director.

The purpose of enhancing the CI personnel was to more adequately handle the threat from foreign nationals and to coordinate the creation, procurement, and distribution of effective CI training resources. This is being accomplished by the assignment of two CISAs at each Center, resulting in an increased number of threat briefings and additional CI training resources. NASA is encouraged to fully leverage the increased personnel by continuing to expand CI awareness training and resources.

Recommendation 10 (restated in 24a): *NASA should place the CI staff in the Centers into the field Protective Services staff under the ultimate supervision of the Center Director with a dotted line organizational relationship to HQ and also require Center officials to seek the approval of HQ when appointing and evaluating CISAs.* ***NASA implemented actions that respond to the intent of these recommendations.***

[17] Counter Terrorism (CT) was added to the Counterintelligence (CI) Division subsequent to the 2014 Academy Report. As such, this review only pertains to CI activities, and thus CT is not regularly referenced.

The intent of this recommendation was to develop closer working relationships with Center personnel. The 2014 Panel Report revealed disparity in the CI awareness programs across Centers. Although most CISAs were effective in educating Center management, the general population of employees and contractors did not always have the same level of awareness.

NASA determined that the CISAs would function more effectively under the sole management of HQ, without dual supervision of HQ and the Center Director. This determination was made based upon the 2000-2007 experience of placing CISAs under the management of the Center Chiefs of Protective Services (CCPS). During this period the CISAs were assigned various security duties and were unable to work CI matters in a full-time capacity. The Protective Services Chiefs were not trained in CI and were unable to provide professional guidance or a standardized national approach to CI. If the CISAs are to remain under HQ supervision, however, the study team believes that Center Directors should provide input in annual performance appraisals of the center CISAs.

CISAs advised during various interviews that they are now more fully integrated into Center operations, and study team interviews with their Center counterparts support this assertion. One of the CI offices is now more accessible than during the original study and CISAs report increased contact with Center employees. In June, 2014, an Agency-wide message to all NASA employees identified the Lead CISAs in the Centers and at HQ. CISAs now have quarterly meetings with the Center Directors and are more integrated into the Center working groups. An example of successful integration into Center activities is evidenced by a Center Director recommending a CISA for NASA's Exceptional Service Medal for sustained performance. Even though the CISA was an Agency employee rather than a Center employee, he received the award. Another example of Center integration is an information briefing by a CISA offered to NASA employees after the OPM data breach was announced. This voluntary program held in an auditorium, with over 500 NASA employees and contractors participating.

Although the CISAs will remain under the sole management of HQ, sustained efforts will be needed to develop personal relationships with Center personnel who may have CI assessment information to share. As one of the most internationally recognized symbols of American ingenuity and success, NASA is a prime intelligence and terrorism target, and foreign nationals approach employees and contractors through both overt and covert means. Americans often fail to recognize these recruitment approaches at home and abroad, and therefore do not report them. If these personnel hold no clearances and do not visit designated countries[18] or Russia, they might not receive any face-to-face CI awareness briefings or debriefings by CISAs.

Most CISAs have developed effective one-way awareness programs: they provide CI threat information to NASA personnel. By fully developing a two-way CI awareness and collection program that focuses not only on information provided but also on information gained through structured debriefings, NASA can identify specific collection patterns of foreign intelligence services. This will result in an increased number of reports sent to outside agencies for inclusion in Intelligence Information Reports (IIRs).

[18] The designated country list comprises approximately 40 countries that currently pose an increased risk to the national security of the U.S.

As an example of a proactive two-way CI Program, one Center CISA recently initiated a Help Mailbox, where employees can report unsolicited foreign email contacts. If NASA's papers are requested from designated countries or employees are invited to travel to designated countries to present papers, the employees can simply forward the foreign emails to the Help Mailbox. CI briefings/debriefings will then be provided to the employees and CISAs will analyze the unsolicited requests for CI value.

Recommendation 11: *Standardize and enhance the CI Awareness and Education Programs nationally. This includes:*

a) NASA HQ and Centers identifying the information that needs to be protected. Once the threat is clarified, the threat message can be communicated more effectively. ***This recommendation has been implemented.***

CISAs are working with EC personnel to clarify what information needs to be protected and to communicate this information through threat briefings. Although individual Centers have very different missions, the core CI Awareness message concerning the need to protect information is the same throughout NASA.

b) Annual CI awareness training being provided to all personnel, including contractors. There are innovative interactive computer programs that can deliver memorable awareness training to reach employees and contractors both onsite and offsite. ***This recommendation has been partially implemented and is ongoing.***

The CI/CT Division has identified interactive training provided by outside agencies and has also teamed with other NASA offices to offer the following standardized awareness and education programs:

- Mandatory Training for all employees and contractors includes an annual security training module with several CI slides. Completion of this module is required to gain and maintain access to NASA computers.
- Mandatory Training for all employees with clearances is delivered through SATERN. The current training is a Defense Security Service (DSS)-produced training module titled, "Insider Threat Awareness." NASA is encouraged to ensure that this training module is updated instead of shown repeatedly each year. An Export Control and CI/CT Awareness training module is also available on SATERN.
- Quarterly Employee CI training is accomplished through the distribution of Security Connection, a newsletter co-produced by the OPS office and the Office of the Chief Information Officer (OCIO). The newsletter provides awareness briefings for defense industry and government employees. A monthly CI/CT/Cyber Newsletter is distributed electronically to all NASA employees and contractors and is posted on the CI/CT website.

For employees without clearances and for contractors, however, CI awareness and education often depends on the employees' interest and the contractors' Facility Security Officer's (FSO) support, unless foreign travel briefings are required. Some CISAs have developed excellent relationships with the FSOs at their Centers, who can encourage contractors to participate in CI training, but other than several slides contained in a security presentation, CI Awareness training has not reached all contractors.

c) Providing specific, unclassified case examples and effective CI training aids such as movies which can be incorporated into the training to present a program that would capture interest while providing critical information. ***This recommendation has been implemented.***

Some CISAs have shown an FBI-developed video to Center employees, entitled, "The Company Man: Protecting America's Secrets." The video is based on an actual case involving Chinese intelligence and its purpose is to raise awareness of the economic espionage threat. At one Center, this video was shown to over 100 contractors from one company. The monthly CI/CT/Cyber newsletter also features unclassified case examples and is distributed in hard copy and electronic formats to all Centers.

d) Having Center CISAs emphasize the "Insider Threat" to employees and contractors, to include identification of potential threats and the necessity of reporting such threats through formalized channels. ***This recommendation has been implemented.***

Through standardized pamphlets, newsletters, video feeds, outside agency presentations, CISA briefings, and SATERN, the Insider Threat message of employee vulnerabilities and the need for reporting suspicious activities is now widely delivered to NASA Centers. The mandatory training for cleared employees is titled "Insider Threat Awareness." One CISA advised that "Insider Threat" is now the buzzword in the CI Division.

Recommendation 12: *NASA HQ should expand the requirement for travel briefings to include all personnel with foreign travel. Ensure that contractors receive current travel briefings, either through their contracting agency or through NASA online or personal briefings resources.* ***This recommendation has been partially implemented and is ongoing.***

NASA has succeeded in expanding travel briefings but it is difficult to ensure that contractors receive briefings unless they have clearances or they travel to designated countries or Russia, with travel expenses paid by NASA.

In June 2014, NASA HQ sent an electronic message to all NASA employees, both civil servants and contractors, restating the requirement to receive counterintelligence briefings before traveling to designated countries or Russia and to receive debriefings after the travel. The CISAs are not able to mandate travel briefings or track the number of briefings received by contractors whose travel costs are not paid by NASA, however. The FSOs at the contracting companies are not required to hold their

contractors responsible for receiving travel briefings unless the contractors have clearances. Most contractors do not have clearances and therefore do not receive consistent briefings. CISAs do not necessarily learn of contractors' upcoming travel, even if the destinations are to designated countries, unless they are advised of the travel by the FSOs. Some contracting companies support travel briefings and debriefings for their contractors, while some do not. The key to widespread briefings appears to be the strength of the relationship developed between the CISAs and the FSOs.

The CISAs provide voluntary counterintelligence threat briefings for employees and contractors for any foreign travel, either business or personal. NASA has gone beyond the intent of this recommendation by offering to provide travel briefings to family members as well, even for personal travel. An added benefit of the expanded voluntary travel briefings is that an increasing number of Center employees now have personal interactions with the CISAs.

Several CISAs reported that they now emphasize travel briefings as a service provided by CI to help employees rather than simply a requirement. The CISAs also added that Administrator Bolden sets the example by requesting travel briefings for himself and his staff.

Due to the significant differences in the numbers of travelers at the different Centers, some CISAs are able to provide more personal travel briefings and debriefings than others. NASA employees are prime targets, and professional intelligence officers will attempt to elicit information and establish relationships with them, in both designated and non-designated countries. Face-to-face debriefings are, therefore, particularly valuable.

Recommendation 13: *NASA HQ should simplify the CI policies and procedures and minimize the number of entities involved with counterintelligence training so that Security and CI/CT mandates do not overlap. Clarify the NPRs and NPDs to reflect distinct responsibilities.* ***This recommendation has been addressed and is awaiting approval prior to being fully implemented.***

The responsibilities of the CI Division and OPS are now more clearly delineated. The CISAs have sole responsibility for the CI Awareness Program as well as for briefing and debriefing travelers and foreign visitor escorts.

The policies and procedures for the CI Program are now consolidated in one revised NPR, 1660.1C: NASA Counterintelligence and Counterterrorism. Center CISAs were invited to provide input, which was used in the final revision. One CISA reported that the consolidated CI policies and procedures are now much more centralized than at his previous military intelligence position, where the policies were scattered. Inconsistencies between NPRs 1660.1 and 1600.4 have been identified. NPR 1600.4 is in the final stages of approval and, when it is signed, this recommendation will be fully implemented.

Recommendation 18: *Develop training modules that clearly indicate the threats that exist and that are specific enough to convince highly educated and sophisticated users of information—such as NASA scientists and engineers—of the risks and dangers. Training should be mandatory with consequences for those who choose not to attend.* ***This recommendation has been partially implemented and is ongoing.***

The DSS's training module, "Insider Threat Awareness," is mandatory for employees with clearances. This training is delivered electronically through the NASA learning management system, SATERN. Additional training is addressed under Recommendation 11. Training modules have been developed but consequences for those who do not participate in the training are unclear, as some personnel interviewed had not taken this required training.

Section 4.3: Additional Considerations

Based on the feedback received from NASA Center personnel involved in CI, the study team recommends that NASA consider taking the following actions to enhance the current CI development efforts:

- **Enhance the two-way CI program to focus not only on providing threat awareness briefings, but also on conducting in-depth personal debriefings to gather information on foreign national collection methods.** Now that the CI/CT Division is fully staffed, NASA has the potential to become an innovative leader in the US Intelligence Community. Because of NASA's international brand and the targeting of its employees, NASA is in a unique position to learn specific collection patterns of foreign intelligence services. The analysis of such CI assessment is of critical value to protect NASA assets. Sustained efforts will be needed to continue to develop personal relationships with Center personnel and to forge strong liaison with FSOs to expand the CI Awareness Program to contractors. With a full CI staff, NASA is encouraged to develop a high-level strategic approach to CI Awareness and outreach.

Section 5: IT Security

Section 5.1: Summary

While NASA has not completed its implementation of 2014 Panel Report recommendations regarding IT security, it has implemented the highest risk recommendations or their highest risk elements, including those related to the immediate threat of IT systems assumed to be compromised and the agency CIO's lack of authority and control over Center networks. Work is continuing on projects to further increase control by creating an integrated network infrastructure that will enable centralized management of network security and the automatic application of security protocols across NASA networks.

Section 5.2: Assessment

NASA progress on the 2014 Panel's recommendations related to IT security (6, 7, and 8) is discussed below in order of the risk-based prioritization of recommendations in the 2014 Panel Report (The risk assigned to each recommendation is mapped in Appendix F).

Recommendation 6, *the highest risk recommendation, includes two elements: (1) identify critical IT assets; and (2) create a working group to develop protective measures that balance security with mission efficiency. The first element is the highest risk as it addresses the immediate threat of compromised IT systems called out in the 2014 Panel Report.* ***Implementation of this recommendation is still underway, but its highest risk element has been addressed.***

The OCIO identified and reported all critical IT assets and protective measures to the Office of Management and Budget (OMB) during the Cybersecurity Sprint launched in response to the Office of Personnel (OPM) breach. OMB found no indication of critical vulnerabilities that would warrant an independent audit. However, the OCIO is continuing to further examine its protective measures and working to implement the OMB directive to strengthen authentication, including the installation of PIV-access systems.

The OCIO established a working group ("Tiger Team," including IT, physical security, and mission personnel) that is beginning the task of developing protective measures to enable a position-based risk approach to access management in keeping with OPM guidance. The working group is working with the National Institute of Standards and Technology (NIST) to develop access management standards appropriate to role-based risk determinations.

The working group's efforts are complemented by a two-pronged strategy to enable a position-based risk approach to access management. First, the OCIO is developing an overall data architecture that will allow tagging institutional and mission data. This will provide the OCIO with a greater capability to identify and tag sensitive and mission critical data and enforce appropriate policies and procedures for its access and use. Five of six domains have been completed. Second, the OCIO is cataloguing data owners and developing plans to prevent data loss.

To enhance the protection of assets across NASA, as well as to facilitate mission operations, the Communications Service Office is undertaking two projects in support of the OCIO's Network

Modernization initiative: the External Border Protection Project (EBPro) and the Enterprise Internal Border-Network Access Control (EIB-NAC) Project. The purpose of EBPro is to strengthen protection across NASA against external threats through the deployment of filtering and security devices between NASA and non-NASA networks. At the same time, action is being taken to reduce and consolidate connections with external networks in compliance with the Department of Homeland Security's (DHS) Trusted Internet Connection Reference Architecture. EBPro also is intended to facilitate collaboration among NASA Centers by enabling a secure, enterprise-wide intranet. The purpose of the EIB-NAC project is to help ensure consistent enforcement of remote access requirements through the deployment of a Network Access Control solution that automatically authenticates, assesses, validates, and places network connecting endpoints and users into network zones commensurate with applicable security policy. Both these projects facilitate the effective application of DHS's continuous diagnostic and monitoring (CDM) tool set across NASA networks.

Recommendation 8 *calls for NASA to determine if there were foreign nationals with system administrator access not captured in the NASA Access Management System (NAMS) and remove them. While this recommendation was determined to be lower risk (highest consequence X lowest probability) it relates to the finding—NASA should assume that its IT systems are compromised—that drove Recommendation 6.* ***This recommendation has been implemented. Also, a measure to provide additional security is planned.***

The OCIO identified five foreign nationals with system administrator privileges. All five were captured in NAMS. The access privileges of all five were reevaluated and validated. In addition, the OCIO instituted an annual revalidation process.

To further increase security, the OCIO plans to apply a foreign national "attribute" identifying emails from foreign nationals. Implementation of this measure is planned for the summer of 2016, contingent on final agreement between an employee union and NASA's Office of Human Capital Management.

Recommendation 7*, the second highest risk recommendation, includes two elements: (1) increase the authority and control of the agency CIO over NASA networks and the ability to standardize administrative assets across the agency, especially as it relates to security policies and protecting information; and (2) improve operational linkage between the agency CIO and Center CIOs. More specifically, the recommendation called for a requirement that the agency CIO's endorsement be sought before any field CIO position is filled and that the agency CIO have input into the annual rating of field CIOs.* ***This recommendation has been partially implemented.***

NASA's actions to increase the authority and control of the agency CIO and to improve operational linkage with field CIOs extend beyond what was called for in the 2014 Panel Report recommendation. Actions include:

- Center CIOs were made direct reports to the agency CIO;

- The agency CIO was given has hiring authority for all Center CIOs (the new CIO has already hired five new CIOs);
- The CIO was made the rating official for all Center CIOs and works with the Center Directors to develop comprehensive assessments of each CIO's performance; and
- To help further improve the linkage between the Agency CIO and Center CIOs, the OCIO has established a CIO Leadership Team, including all the Center CIOs and Agency OCIO senior staff.

The authority and control of the agency CIO have been enhanced by OCIO's actions to satisfy prior Office of the Inspector General (OIG) recommendations and to comply with the requirements of FITARA,[19] which was enacted following the 2014 Panel Report.

- The OCIO has completed actions on an overlapping and complementary set of recommendations issued by the OIG in a 2013 audit of IT governance at NASA. All these recommendations have been officially closed; and
- The OCIO has almost completed plans for implementing measures to comply with FITARA requirements. OMB approved its FITARA Implementation Plan, and the agency's Mission Support Council will review its revised Baseline Services Assessment plan in late March 2016.

Standardizing administrative assets and fully realizing the control over network security that this will enable is a more difficult and longer-term task that the OCIO is continuing to address through its "network transformation" initiative. This initiative includes two projects currently underway.

- The Consolidated Network Operations Services (CNOS) project. The CNOS project aims to centralize the management of NASA's corporate and Center networks that will facilitate the enterprise-wide application of DHS' continuous diagnostics and monitoring tool set; and
- The Mission Backbone Transition (MBT) project. The MBT project aims to place corporate and mission network on a common backbone infrastructure, which will enable improved security as well as efficiency.

[19] Federal Information Technology Acquisition Reform Act (FITARA) was enacted on December 19, 2014. FITARA outlines specific requirements related to: (1) Agency Chief Information Officer Authority Enhancements; (2) Enhanced Transparency and Improved Risk Management in IT Investments; (3) Portfolio Review; (4) Federal Data Center Consolidation Initiative (5) Expansion of Training and Use of IT Cadres; (6) Maximizing the Benefit of the Federal Strategic Sourcing Initiative; and (6) Government-wide Software Purchasing Program.

Appendix A: Expert Advisory Group and Study Team Bios

EXPERT ADVISORY GROUP

Karen Evans*— National Director, U.S. Cyber Challenge and Partner, KE&T Partners, LLC. Former Administrator, Office Electronic Government & IT, Office of Management and Budget, Executive Office of the President; Chief Information Officer, U.S. Department of Energy. Former positions at U.S. Department of Justice: Division Director, Information Systems Management, Office of Justice Programs; Staff Director, Computer Services Staff, Justice Management Division. Former Deputy Director, Farmers Home Administration, Applications Management Division, U.S. Department of Agriculture.

Deidre A. Lee*— Independent Consultant. Former: Vice President, Operations Support, Fluor Government Group. Deputy Director of Operations, Federal Emergency Management Agency; Assistant Commissioner for Integrated Technology Service, General Services Administration; Director, Defense Procurement and Acquisition Policy, Office of the Secretary of Defense, ; Administrator, Office of Federal Procurement Policy, Office of Management and Budget; Associate Administrator for Procurement and Executive Officer to the Deputy Administrator, National Aeronautics and Space Administration.

Barbara Romzek*— Barbara Romzek is an internationally recognized scholar of public affairs. She joined American University as Dean of the School of Public Affairs in 2012 after holding several leadership positions at the University of Kansas. Dr. Romzek is an expert in the areas of public management and accountability, with emphases on government reform, contracting, and network service delivery. She has conducted research that has encompassed complex work settings, including NASA, Congress and the Air Force, as well as state agencies, local governments and nonprofit agencies. She has received research awards from the American Political Science Association and the American Society for Public Administration. She has served on the governing boards of the American Political Science Association and currently serves on the executive council of the Network of Schools of Public Affairs and Administration. Dr. Romzek is the co-author of three books and scores of journal articles, book chapters and other publications

STUDY TEAM

Joseph P. Mitchell, III, *Director of Academy Programs*: Dr. Mitchell leads and manages the Academy's studies program and serves as a senior advisor to the Academy's President and CEO. He has served as Project Director for past Academy studies for the Government Printing Office, the U.S. Senate Sergeant at Arms, USAID/Management Systems International, the National Park Service's Natural Resource Stewardship and Science Directorate, and the USDA Natural Resources Conservation Service. During his 15 years at the Academy, Dr. Mitchell has worked with a wide range of federal cabinet departments and agencies to identify changes to improve public policy and program management, as well as to develop practical tools that strengthen organizational performance and assessment capabilities. As the Academy's studies director, he has provided executive-level leadership, project oversight, and subject matter expertise to over 40 highly regarded organizational assessments, consulting engagements, and thought leadership efforts. He served on prior Academy studies for NASA, including an evaluation of the agency's technology transfer efforts, workforce management, and organizational structure. He holds a Ph.D. from the Virginia Polytechnic Institute and State University, a Master of International Public Policy from The Johns Hopkins University School of Advanced International Studies, a Master of Public

Administration from the University of North Carolina at Charlotte, and a B.A. in History from the University of North Carolina at Wilmington.

Roger Kodat, *Project Director*: Mr. Kodat has led nine projects at the Academy on a range of planning and operational matters. He brings 20 years of commercial and investment banking experience with JPMorganChase, and six years of senior level federal government experience at the Department of the Treasury. He was appointed Deputy Assistant Secretary of Treasury, responsible for Federal Financial Policy in 2001. His tasks at Treasury included rule-making and oversight of Federal loan and loan guarantee programs; and managing the Federal Financing Bank (a $32 billion bank at that time). Previously he served as an Advisor to Treasury's Office of Technical Assistance on international finance projects undertaken in the Czech Republic. He was Vice President and Senior Country Officer for the Chase Manhattan Bank in Prague for several years, managing relationships, setting strategy and executing over $3 billion of corporate finance transactions for the Bank's Czech and Slovak clients. He also was the principal advisor to the Chairman of Komerční Banka, the largest bank in the Czech Republic, from 1991-1993. He served as liaison to the bank's international accounting firm and multilateral development banks, helped introduce standards of integrity in transactional decision-making, and oversaw the bank's first international audit. For ten years, he was Vice President and Group Head, Eastern Europe/USSR, for Manufacturers Hanover Trust Company. He was responsible for client relations, credit risk management and a portfolio of more than $750 million in a region that included Bulgaria, Czechoslovakia, Hungary, Poland, Romania, Russia, and Yugoslavia. Mr. Kodat holds a BS in Education from Northwestern University and both an MBA in Finance and MA in Political Science from Indiana University.

Susan Adams, *Senior Advisor:* Dr. Adams is a retired FBI Agent who taught in the FBI's Counterintelligence Training Center both before and after retirement and served as a senior advisor on the Academy's previous foreign national access management review for NASA. She also supervised the FBI Academy Unit in charge of investigative interviewing instruction and co-founded the FBI's Behavioral Analysis Program. As an Adjunct Associate Professor, Dr. Adams currently teaches Criminal Justice Management in the Graduate School of the University of Maryland University College and Counterintelligence courses for the Intelligence Community. She has authored over a dozen articles published in international journals, books, and law enforcement publications, and addressed international conferences in Vienna, Prague, Edinburgh, Ottawa and Toronto. She earned her Ph.D. in Human Development from the Virginia Polytechnic Institute and State University, and received the University of Virginia's Jefferson Award for excellence in research for her study, "Communication under Stress: Indicators of Veracity and Deception."

John Martinez, *Senior Advisor:* Mr. Martinez has extensive worldwide security and international trade experience acquired through government and private sector executive assignments that span a career of more than four decades. He served as a senior advisor on the Academy's previous foreign national access management review for NASA. In 2011, he completed a one-year project as an associate monitor and special compliance officer, in support of the Independent Monitor and Special Compliance Official (SCO) for the U.S. Department of Justice and U.S. Department of State. Utilizing his federal enforcement expertise, Mr. Martinez assisted with the monitoring of a specific defense company's compliance with the Arms Export Control Act (AECA), International Traffic in Arms Regulations (ITAR), and U.S. programs directed at the protection of sensitive and classified information as well as technology. Mr. Martinez supported the oversight of all corporate policies and procedures related to the ITAR and developed strategies for the protection of sensitive and classified information. Following firsthand inspections of many of the company's domestic facilities, Mr. Martinez co-wrote reports with the Independent Monitor that communicated his findings, conclusions, and recommendations, and ensured strict

compliance with all aspects of government regulations. Before entering the private sector, Mr. Martinez had a distinguished career in the federal service, primarily with the United States Customs Service's Office of Investigations, but also within the Department of State and on Capitol Hill. His last two Customs Service assignments were as the Agent in Charge of the Washington Field Office and as the U.S. Customs Attaché in the American Embassy, London, England.

Joseph Thompson*, *Senior Advisor (and Academy Fellow):* Mr. Thompson is the President, Aequus Inc., a management consulting company. He was the project director for the Academy's previous foreign national access management review for NASA. A retired federal executive, Thompson had a distinguished career at the U.S. Department of Veterans Affairs, serving as the Undersecretary for Benefits, U.S. Department of Veterans Affairs, Washington, DC; Director of the VA Regional Office; Assistant Director of the VA Regional Office and Insurance Center, Philadelphia, PA; Administrative Officer at the Central Office in Washington, DC; and as a Veterans Claims Examiner in the VA Regional Office of New York.

Nicole Camarillo, *Project Advisor*: Ms. Camarillo is the Associate General Counsel and Project Development Advisor for the National Academy of Public Administration. Nicole has a legal background in regulatory compliance and employment law issues. She has extensive experience working for nonprofits on a variety of advocacy issues and has federal campaign experience. At the Academy, Nicole assists the Academy's General Counsel on all employment law and policy matters affecting the organization. She also serves as a legal advisor on Academy studies, particularly those involving legislative and regulatory matters, including the recent reviews for the U.S. Department of Justice's Civil Rights Division and the National Science Foundation. She assists the Director of Academy Programs with the development of Academy proposals and studies. Ms. Camarillo received her B.A. from Stanford University and her J.D. from the University of California, Berkeley School of Law.

Jon Tucker, *Project Advisor*: Dr. Tucker joined the Academy's staff in 2004 and is a Senior Analyst with expertise in policy analysis, program evaluation, organizational design and management assessment, strategic planning, and information technology (IT) management. He was the lead analyst for IT issues for the Academy's recent assessments for the Department of Housing and Urban Development and the Social Security Administration. He holds a Ph.D. in Public Policy from George Mason University, an M.S. in Science and Technology from Rensselaer Polytechnic Institute and a B.A. in Public Policy from New College of the University of South Florida.

Harrison Redoglia, *Senior Research and Communications Associate*: Mr. Redoglia joined the Academy in 2014. He served on the Academy's project examining the Office of Inspector General of the U.S. Department of State, the Federal Leaders Digital Insight Study, and a study that provided recommendations to enhance the role of the federal government in cybersecurity education. He has also assisted with Academy studies of GAO's high risk areas and Governance of Cybersecurity, in addition to serving as the lead staff on the Academy's Transition 2016 initiative. He holds a B.A. in political science from Southern Methodist University.

**Academy Fellow*

Appendix B: Interview List

Ames Research Center

Cohen, Jacob—Chief Scientist

Davis, Jerry—Chief Information Officer

Frost, Chad—Area Lead, Autonomous Systems and Robotics

Hower, Wende—International Visit Coordinator

Knoth, Chris—Lead Counterintelligence Special Agent

Lee, Katharine—Assistant Branch Chief, Terminal Area Air Traffic Management Research Branch

Munar, Lori-Ann—Publications Specialist/STI Manager

Silverman, Kenneth—Chief of Security

Williams, Mary—Center Export Administrator

Armstrong Flight Research Center

Sutton, Frank—Lead Counterintelligence Special Agent

Center for Counterintelligence and Security Studies

Major, David—President

Federal Bureau of Investigation

Morgan, Michael—Counterintelligence Liaison, Houston

Glenn Research Center

Crawford, George—Lead Counterintelligence Special Agent

Goddard Space Flight Center

Aleman, Roberto—MMS Observatory Manager

Breil, Christian—Lead Counterintelligence Special Agent

Durning, John—Deputy Project Manager, James Webb Space Telescope Project

Frost, Jim—Business Specialist

Martin, Eugene—Deputy Project Manager

Weisz, Thomas—Center Export Administrator

Headquarters

Cahoon, Leslie—ICAM Service Executive, Office of the CIO

Condes, Al—Assistant Administrator for International and Interagency Relations

Conroy, Terry—Acting Director for Enterprise Services and Integration

Dahlgren, Jennifer—Support Contractor, Export Control Program

Flynn, David—Export Administrator

Hall, John—Director, Export Control and Interagency Liaison Division

Lightfoot, Robert—Associate Administrator

Mahaley, Joe—Assistant Administrator for Protective Services

Meidinger, Jolene—Foreign National Access Management Program Manager

Morgan, Stefan—Counterintelligence Cyber Agent

Nicholas, James Paul—Agency Identify Management Official

Payton, Art—Regional Counterintelligence Director

Saxon, Kim—Regional Counterintelligence Director

Slone, Darrell—Counterintelligence Division Director

Jet Propulsion Laboratory

Aden, Randy—Manager, Office of Protective Services

Butler, Christopher—Investigations Group Supervisor

Delatorre, Mabel—International Visit Coordinator

Israelsson, Ulf—Euclid Project Manager

James, Keyla—International Visit Coordinator

Kim, Yunjin—Project Manager

Mase, Robert—Project Manager

Odum, Terry—Chief of Protective Services

O'Malley, J.J.—Lead Counterintelligence Special Agent

Roberts-Owens, Dale—Audit Liaison

Skinner, Rachel—Export Licensing Officer

Sukhatme, Kalyani—Mid-Infrared Instrument Project Manager

Johnson Space Center

Davenport, David—Counterintelligence Special Agent

Dietsch, Tony—Lead Counterintelligence Special Agent

Kennedy Space Center

Storey, Ron—Lead Counterintelligence Special Agent

Langley Research Center

Cagley, Kimberly—International Visit Coordinator

Crawford, James—Principal Investigator

Dee, Kevin—Center Export Administrator

Durand, Annabelle—Computer Engineer

Logan, Roy—Chief of Security

Marchione, Ben—Lead Counterintelligence Special Agent

Ross, Richard—Aerospace Engineer

Ross-Clunis, Monica—Acting Deputy, Center Operations Directorate

Marshall Space Flight Center

Betts, Jason—ICAM Developer

Diehl, Gwen—ICAM Developer

Ewing, Daphne—ICAM Developer

Hopson, Rebecca—International Visit Coordinator

Ing, Sharon—ICAM Project Manager

Miller, Nikki—ICAM Product Delivery Manager

Nabors, William "Rip"—Center Export Administrator

Posey, Phil—IT Specialist

Smith, Ron—Lead Counterintelligence Special Agent

Swann, Duffy—ICAM Developer

Wilson, Michael—Chief of Protective Services

Office of the Inspector General

Small, Vincent—JSC Project Manager, Information Technology

Tolomeo, Raymond—Director, Science and Aeronautics Research

Stennis Space Center

Malcom, Dave—Lead Counterintelligence Special Agent

Appendix C: Findings and Recommendations from 2014 Panel Report

#	*FINDING*	RECOMMENDATION
1.	*NASA FNAM guidance often does not provide specific direction as to the process that should be followed and the steps that should be taken.*	HQ staffs should write a detailed operating manual that incorporates all FNAM elements into a comprehensive "how to" manual to guide Center staff through the specific steps of the entire FNAM process. Headquarters staff should work in consultation with knowledgeable field staff in creating this manual.
2.	*FNAM NPRs are often ignored by field Center staff who instead substitute word-of-mouth and locally-developed procedures.*	NASA should significantly reduce the flexibility for Centers to change aspects of the FNAM system by developing the manual mentioned above coupled with a better means for determining whether these instructions are being followed and measuring the outcomes for the processes. Recommendation 21 proposes a compliance and audit mechanism for how this can best be accomplished.
3.	*There is inconsistent application and compliance with established policies and broad interpretation of the NPRs regarding remote access.*	NASA HQ should establish clear, specific, and mandatory requirements for all Centers to follow regarding remote access. This should be incorporated into a broader effort to create a FNAM manual as described in Recommendation 1.
4.	*IdMAX business processes and workflows do not currently support all FNAM requirements. All stakeholders, including end-users, need to be represented in its business process redesign.*	IdMAX business processes should be enhanced to include all FNAM requirements, including an electronic Technology Transfer Control Plan (TTCP) that automatically limits access to systems and assets based on specific criteria selected. A review of the current business processes should be conducted by a team consisting of representatives from all NASA ICAM stake holders at both the Centers and Headquarters. Center staff from all disciplines in the identity management and credentialing process, including sponsors, hosts and escorts, should be allowed to provide input.
5.	*Visual Compliance is an adequate initial vetting tool, but NASA Headquarters has not provided guidance to the Centers on how to respond if they receive a positive response to an inquiry.*	NASA HQ staff should develop procedures and protocols to follow when a positive "hit" is obtained in a Visual Compliance check. This should be incorporated into a broader effort to create a FNAM manual as described in Recommendation 1.
6.	*There is widespread concern among IT professionals and information owners that the NASA IT systems have been compromised. NASA has not adequately identified its sensitive or proprietary data.*	NASA leaders should assume that sensitive data on the networks have been compromised and determine what critical information needs to be protected. NASA should establish a working group to determine the best methods for protecting this information in a manner that does not prevent system owners from being able to meet their mission needs.

7.	*Headquarters and Center CIOs lack authority and control over the networks and are unable to enforce the implementation of IT security programs on most of NASA's IT assets regarding Foreign National Access Management. Decentralization gives NASA Center system owners too much autonomy, leading to ineffective management.*	NASA should reduce the autonomy of the Center CIOs and system owners. HQ CIO needs more authority and control over mission networks and the ability to standardize administrative assets across the Agency, particularly as it relates to security policies for protecting information. Field Center CIOs should be more closely linked to the HQ CIO operation, including the requirement that a HQ endorsement be sought before any field CIO job is filled and that the HQ CIO be provided input into each field CIO annual rating. The Panel acknowledges the 2010 memo from the Administrator that states the Center CIOs will report to the HQ CIO, but notes that the memo does not specifically provide details regarding hiring endorsements or performance input.
8.	*It is difficult to determine if there are more individuals with system administrator privileges than necessary.*	NASA should continue efforts to review the number of system administrators and limit the number to those who actually need such access. NASA should determine if there are foreign nationals with privileged access to the NASA systems that are not captured in NAMS and if so, remove them from that role.
9.	*The current number of personnel assigned to the CI/CT Program is inadequate to formulate, manage, and perform effective CI Awareness and Education programs.*	NASA should increase the number of CI personnel to adequately handle the threat from foreign nationals and to coordinate the creation, procurement, and distribution of effective CI training resources.
10.	*Center-based CISAs would function more effectively if placed under Center management with close HQ oversight.*	NASA should place the counterintelligence staff in the Centers into the field Protective Services staff under the ultimate supervision of the Center Director with a dotted line organizational relationship to HQ and also require Center officials to seek the approval of HQ when appointing and evaluating CISAs.
11.	*The effectiveness of the NASA CI Awareness and Education program varies greatly among the Centers, with some being ineffective.*	Standardize and enhance the CI Awareness and Education Programs nationally. This includes: a) NASA HQ and Centers identifying the information that needs to be protected. Once the threat is clarified, the threat message can be communicated more effectively. b) Annual CI awareness training being provided to all personnel, including contractors. There are innovative interactive computer programs that can deliver memorable awareness training to reach employees and contractors both onsite and offsite. c) Providing specific, unclassified case examples and effective CI training aids such

		as movies which can be incorporated into the training to present a program that would capture interest while providing critical information. d) Having Center CISAs emphasize the "Insider Threat" to employees and contractors, to include identification of potential threats and the necessity of reporting such threats through formalized channels.
12.	*The CI travel briefing program appears to have the most consistency and clarity of the CI programs, but it reaches only a limited number of personnel.*	NASA HQ should expand the requirement for travel briefings to include all personnel with foreign travel. Ensure that contractors receive current travel briefings, either through their contracting agency or through NASA online or personal briefings resources.
13.	*The policy and procedures for CI awareness and education overlap within OPS Divisions.*	NASA HQ should simplify the CI policies and procedures and minimize the number of entities involved with counterintelligence training so that Security and CI/CT mandates do not overlap. Clarify the NPRs and NPDs to reflect distinct responsibilities.
14.	*NASA Headquarters (HQ) Officials and Center Directors have not adequately communicated that strict compliance was and is required for foreign national hosting, sponsoring, and escort policy and procedures.*	NASA HQ leadership and Center Directors should periodically and formally reiterate to all employees and contractors the importance of Security and CI/CT Programs and functions, and each individual's responsibility to support them. The best practices utilized by other agencies to train, guide, direct, and assess personnel involved in FNAM procedures should be evaluated for use by NASA.
15.	*There is little uniformity and consistency in the application of the procedural requirements for hosts/sponsors and escorts among the Centers. This includes briefings and debriefings, the documents used to delineate the physical and/or logical access plans, and the duties and responsibilities of those involved in the process.*	To ensure uniformity and consistency, OPS should develop standardized Security and CI awareness and training materials; briefings for sponsors, escorts, and visitors; and forms pertaining to the FNAM process. The "best practices" developed and utilized by other agencies to include procedural requirements, training, education, and programmatic evaluation should be leveraged and implemented when appropriate.
16.	*Foreign National Access Management (FNAM) procedures, particularly those for*	NASA HQ organizations involved in the FNAM process (OPS, OIIR, OCIO) should jointly produce simplified and standardized, step-by-step procedural instructions for each functional component

	individuals from Designated Countries and high-threat locations, are considered by requesters, sponsors, and escorts to be too complex, confusing, and time-consuming. This has created a reluctance or refusal to utilize the expertise and skills of foreign nationals by some NASA sponsors.	comprising the process for use by affected personnel. This procedure should be incorporated into a broader effort to create an FNAM "manual" as described in Recommendation 1.
17.	*The Integrated Functional Reviews and CI/CT Evaluations do not specifically address the performance of the tasks pertaining to hosting/sponsoring and escorting foreign nationals.*	The periodic Integrated Functional Reviews and CI/CT Program Reviews conducted at NASA Centers should be expanded to assess and evaluate the procedural components comprising the FNAM process to include their effectiveness and efficiency. This evaluation should be incorporated in the creation of Independent Review Teams as described in Recommendation 22.
18.	*The required briefings of sponsors and escorts of foreign nationals have not adequately conveyed the risk the individual might pose to NASA assets.*	Develop training modules that clearly indicate the threats that exist and that are specific enough to convince highly educated and sophisticated users of information – such as NASA scientists and engineers – of the risks and dangers. Training should be mandatory with consequences for those who choose not to attend.
19.	*The Export Control program needs a more standardized and systematic approach in furtherance of its export compliance objectives, as well as better audit and review mechanisms. NASA senior leaders also need to more strongly endorse the critical importance of such controls.*	NASA should take steps to systematize the approach to export control and emphasize its importance by: a) Providing a detailed export control manual that will serve as a standardized guide to Center CEAs, ECRs and Center project managers and mandate the use of certain practices that have proven effective at various centers (use of ECRs, ECCs, and scrubbed laptops for travel are a couple). This export control manual should then be incorporated into a broader effort to create an FNAM "manual" as described in Recommendation 1. b) Issuing a strongly-worded communication from senior management to NASA employees that affirms the Agency's commitment to export compliance, explains the basic purpose of export controls, directs employees to comply with export laws and regulations, states the potential penalties for non-compliance and identifies individuals to contact for further information. c) Conducting outside periodic reviews of the each Center's export control activities to assess and

		evaluate the procedural components, to include their effectiveness and efficiency. This should be incorporated in the creation of Independent Review Teams as described in Recommendation 22. d) Requiring that a HQ endorsement be sought before any field CEA job is filled and that the HQ export control organization provide input into each field CEA annual rating to strengthen the linkage between Center CEAs and their HQ counterparts.
20.	*Export control training requirements are inconsistent; the training is confusing and inadequate; and the rationale for such training is often poorly understood.*	NASA should revisit its current export training program and develop an improved and more effective, standardized training program for educating both specialized Center export control personnel as well as other NASA employees who need to understand US export regulations.
21.	*FNAM is not managed as a program. The responsibility for various elements are "stovepiped" with no overall process owner among the NASA HQ organizations.*	NASA should formally establish FNAM as a program within OPS and appoint a single program manager to oversee it.
22.	*NASA needs more robust mechanisms for ensuring that FNAM policy requirements are being met by field Centers.*	Create an Independent Review Team, led by the Office of Protective Services, and including membership for OIIR and CIO and field Center representatives, to biennially review all field Centers to assess and evaluate the procedural components comprising the asset protection program to also include effectiveness and efficiency. The team should operate under the guidance of the Asset Protection Oversight Board.
23.	*NASA needs to reconsider how it assesses and protects its information and security assets in the field.*	Create an Asset Protection Oversight Board to oversee the safety and security of NASA assets in the field. The overall goal of the Board is to protect all of NASA's valuable ITAR and EAR technical data and proprietary information, not simply the data potentially exposed to foreign nationals and to also compile threat assessments from security, CI/CT, and the CISOs into comprehensive Center and agency threat/risk assessments. These assessments could be incorporated into NASA's risk management process. The Board should be supported by the HQ OPS.
24.	*There are a several organizational changes NASA can make to strengthen FNAM.*	The Panel recommends the following: a) Placing the counterintelligence staff in the field into the field Protective Services staff under the ultimate supervision of the Center Director. b) Elevating the organization with the primary responsibility for Foreign National Access Management – Protective Services in NASA Headquarters – onto a level with more direct

		reporting responsibilities to the Office of the Administrator to ensure that these critical issues receive the appropriate amount of leadership attention. The Panel believes that more visibility for HQ OPS coupled with a stronger relationship with field counterparts will help to strengthen NASA's overall security. c) Forging stronger organizational relationships between certain key FNAM-related jobs in the field, specifically the Center Export Administrators and Counterintelligence Special Agents with their HQ counterparts. Creating a strong linkage (a "dotted-line" organizational relationship) between the HQ and field entities can only strengthen FNAM. If adopted by NASA, this would mean that Center Directors must seek the endorsement of these HQ officials before appointing anyone into these positions. The input of the HQ officials should also be included in the annual evaluations of individuals holding these FNAM-related jobs in the field.
25.	*NASA needs to take steps to reduce the decentralized authority given to Centers for implementing FNAM and other largely procedural or enterprise-wide processes.*	The Panel believes that implementation of the other recommendations in this review will help to resolve this issue; therefore, no recommendation is made for this finding.
26.	*Unnecessary competition between Centers is counterproductive.*	NASA leaders in both HQ and the field need to promote cooperation as opposed to competition between field Centers and encourage and facilitate sharing of best practices and FNAM capabilities.
27.	*Culture plays an important role in every aspect of NASA operations, and for FNAM, some aspects of the culture are disadvantageous*	Hold individuals accountable when they make serious, preventable errors or deliberately fail to follow important FNAM guidelines, procedures or requirements. Without a system of accountability, there is little likelihood of success in improving FNAM. Additionally, NASA leaders need to guard against the Agency's tendency to gradually revert back to previous behaviors once the immediacy of a problem has passed. Establishing the compliance and asset protection mechanisms recommended earlier will help with this solution.

Appendix D: Executive Summary of 2014 Panel Report[20]

EXECUTIVE SUMMARY

"Expand international cooperation on mutually beneficial space activities to: broaden and extend the benefits of space; further the peaceful use of space; and enhance collection and partnership in sharing of space-derived information"

— A Goal of the National Space Policy of the United States of America - June 28, 2010

The National Aeronautics and Space Administration (NASA) is one of the most accomplished agencies in the U.S. federal government and one of the most respected government entities in the world. To accomplish its mission, NASA works collaboratively with many nations on a broad range of scientific and engineering projects. Foreign national participation in NASA programs and projects is an inherent and essential element in NASA operations. No better illustration of this partnership is the fact that during 2013, NASA's international operations were being supported by over 600 cooperative agreements with 120 nations.

Having a well-run Foreign National Access Management program is in the best interests of NASA, both in terms of protecting vital U.S. security and proprietary information, as well as capitalizing on the talents of foreign nationals. This Academy review examined the Agency's entire FNAM process from the initial request from a requestor or sponsor through foreign national vetting, credentialing, information technology security, counterintelligence, hosting and escort procedures, and export controls.

There is a fundamental tension between NASA's charter to work cooperatively and share information with other nations while simultaneously safeguarding its sensitive and proprietary information and assets from those same nations. How well NASA is able to balance these sometimes conflicting demands and what it might do to improve its processes for working with foreign nationals are the principal questions addressed in the Academy's review.

Over the last year, security incidents involving foreign nationals at NASA research Centers have drawn the attention of the NASA Administrator and other agency leaders, Congress, and the media. Recognizing the growing threat of cyber-attacks and espionage aimed at government agencies by hostile nation-states and foreign adversaries, NASA asked the National Academy of Public Administration (the Academy) to conduct this review of its foreign national management processes.

NASA staff members are dedicated, knowledgeable, committed to the mission, and genuinely happy to be working for NASA — they routinely rank the Agency as the best place to work in the federal government. NASA interviewees for this study were candid, cooperative, and eager to both offer suggestions and be involved in problem solving. Most NASA employees understood the challenge to share with, as well as to protect information from foreign nationals.

[20] The final report was not made public due to a determination that it contained confidential information. Only the Executive Summary is available to the public.

Having such a high-quality, dedicated workforce is a tremendous advantage for NASA in pursuing any improvement initiatives.

The Academy Panel found that as with many federal agency programs, budget and personnel cuts have made the management of NASA's security programs difficult. The Panel is sensitive to the budget situation NASA faces and has tried to keep most of its recommendations within achievable budget limits although some may prove to be resource-intensive. The Panel also thinks that strong leadership, which it believes NASA has, can accomplish much of what is recommended within existing resource limitations. In addition to the mission and security improvements that can be achieved, there are also long-term potential savings the Agency can realize by managing its foreign national efforts in a more efficient and effective manner.

Despite the resource constraints, NASA leaders have already taken a number of positive steps to correct some of the weaknesses in the Foreign National Access Management (FNAM) process, including a moratorium on foreign national access which required each NASA field Center to evaluate its respective compliance with FNAM procedural requirements, a process completed earlier this year. Requesting this Academy review also demonstrates NASA's commitment to making improvements to improving FNAM. To build on NASA's goals, the Panel believes there are a number of important steps the Agency can take to improve FNAM and has proposed twenty-seven recommendations, the most significant of which are combined under the following six topics:

1. **Managing Foreign National Access Management as a Program** – Currently, FNAM is not managed as a program. There is no systematic approach to FNAM at NASA; rather, there are individual Headquarters program requirements coupled with individual NASA Center approaches. Given inadequate means for determining the overall effect of these processes, the result is a broad range of outcomes, many of which are insufficient. The following steps towards a coordinated FNAM program would begin to coordinate efforts and secure better results:

a. Change FNAM organizational alignments and reporting requirements in NASA Headquarters and field Centers. This restructuring includes moving counterintelligence staff from under the direct supervision of the HQ Office of Protective Services to the supervision of field Centers; moving the Office of Protective Services in HQ up one level to provide a more direct relationship between the Office and NASA senior leaders; and strengthening the formal organizational relationships between individual field Center FNAM staff and NASA HQ program staff.

b. Improve training by developing comprehensive, integrated curriculums and lesson plans. This training would include all of the components of the FNAM process such as export control, host, sponsor, escort and counterintelligence.

2. **Reducing the flexibility given to Centers to interpret FNAM requirements** – Too much flexibility in largely procedural processes coupled with a "stovepiped" organizational structure and overly broad and organizationally-specific directives has resulted in inconsistent and ineffective outcomes. The following steps should be taken by NASA Headquarters:

a. Write a comprehensive and detailed FNAM operating manual covering all functional aspects of the program. Headquarters staff should work in consultation with knowledgeable field staff in creating this manual.

b. Conduct periodic, external, programmatic reviews of field Center FNAM to include a focus on overall performance and asset protection.

3. **Determining critical assets and building mechanisms to protect them –** NASA needs to improve how it protects all of its valuable technical data and proprietary information, not simply the proprietary, sensitive, and/or classified information potentially exposed to foreign nationals. Building on existing Agency risk review processes, NASA should require each Center to prepare and submit a comprehensive assessment of threats to its facilities, personnel, technologies, and information in order to compile an agency-wide threat/risk assessment. The following steps should be taken by NASA HQ:

a. Establish an Asset Protection Oversight Board to manage the overall effort.

b. Create an Independent Review Team to review the individual program compliance metrics, the overall performance and outcomes of FNAM, and the adequacy of the comprehensive threat/risk assessment at each Center.

4. **Correcting longstanding information technology security issues –** Given the extent of the concerns expressed during this review by NASA IT professionals regarding the security of the Agency's non-classified systems, the Agency should:

a. Establish a working group to identify and protect sensitive, proprietary information in a manner that does not prevent system owners from meeting their mission needs.

b. Establish clear, specific, and mandatory requirements for all Centers to follow regarding remote access of their information technology systems.

c. Give the NASA Chief Information Officer more control over IT operations in field Centers.

5. **Changing several aspects of NASA culture –** In most ways, NASA has an excellent organizational culture, but several factors need to be addressed when considering how best to improve FNAM:

a. Decrease the competitiveness, and correspondingly, increase cooperation between Centers. This dynamic can create an inflection point for needed change at NASA well beyond the issue of foreign national access management.

b. Improve accountability, particularly when serious mistakes are made or mandates are ignored; this is essential to improving the systems of management controls.

c. Guard against the tendency to revert back to prior lax habits once a problem has been solved and the tension of the moment has passed.

6. **Communicating the importance of these changes clearly, firmly and consistently –** The importance of security, the existence of "real world" threats to NASA assets, and the need for

improvements in handling foreign national issues have not been clearly and consistently communicated throughout NASA. Senior leaders must firmly establish and communicate their total commitment to an effective FNAM program that enhances cooperation while safeguarding information.

Appendix E: Foreign National Access Management Stakeholder Engagement Detail (Provided by NASA)

NASA FNAM Stakeholder Engagement Detail			
Meeting/Working Group	**Frequency**	**Purpose**	**Attendees (role/responsibility)**
International Visit Coordinator (IVC) Teleconference	Monthly (2014 – 2015) Quarterly (2015 – Present)	Provide FNAM Program updates to Center IVCs. Discuss topics of interest and/or provide requested training on specific topics.	Center IVCs, FNAM Program Manager, FNAM Project Managers (as requested), FNAM Support Staff
Center Chiefs of Protective Services Teleconference	Monthly (2014 – Present)	Provide FNAM updates to Center Chiefs of Protective Services.	Center Chiefs of Security, OPS Senior Leadership (Assistant Administrator, Deputy Assistant Administrator, and others as appropriate)
FNAM Project Manager Meeting	Monthly (2014 – Present)	Provide FNAM Program updates to FNAM Project Managers. Discuss topics of interest and updates in each stakeholder office.	FNAM Project Managers from OPS, OIIR, and OCIO
FNAM Program: Internal Outreach	As needed	Provide outreach to internal programs with interest in or impacted by FNAM. Provide guidance and explanation of requirements regarding FNAM.	Office of Education, Office of Procurements/Grants
FNAM Program: External Outreach	Activities in response to external requests	Provide outreach to external programs to provide advice, guidance, and lessons learned for implementation and execution of an FNAM program.	Department of Commerce, National Institute of Standards and Technology (NIST), Department of Interior, National Science Foundation (NSF)
Quarterly Export Control Program Video Conferences	Quarterly (2013 – Present)	Provide opportunity to update Center Export Control Staff on regulatory changes, programmatic changes, new initiatives, provide topic specific training delivered by guest speakers or HQ Export Control Staff, and solicit issues and concerns from the Center Export Control Staff	Center Export Administrators, Alternate Center Export Administrators, Center Export Counsels, program Export Control Representatives, other Center Export Control support staff
Annual Export Control Program Review	Annually (1995 – Present)	Review compliance activities of the previous year, review progress towards addressing issues and concerns raised during	Center Export Administrators, Alternate Center Export Administrators, Center Export Counsels, program Export

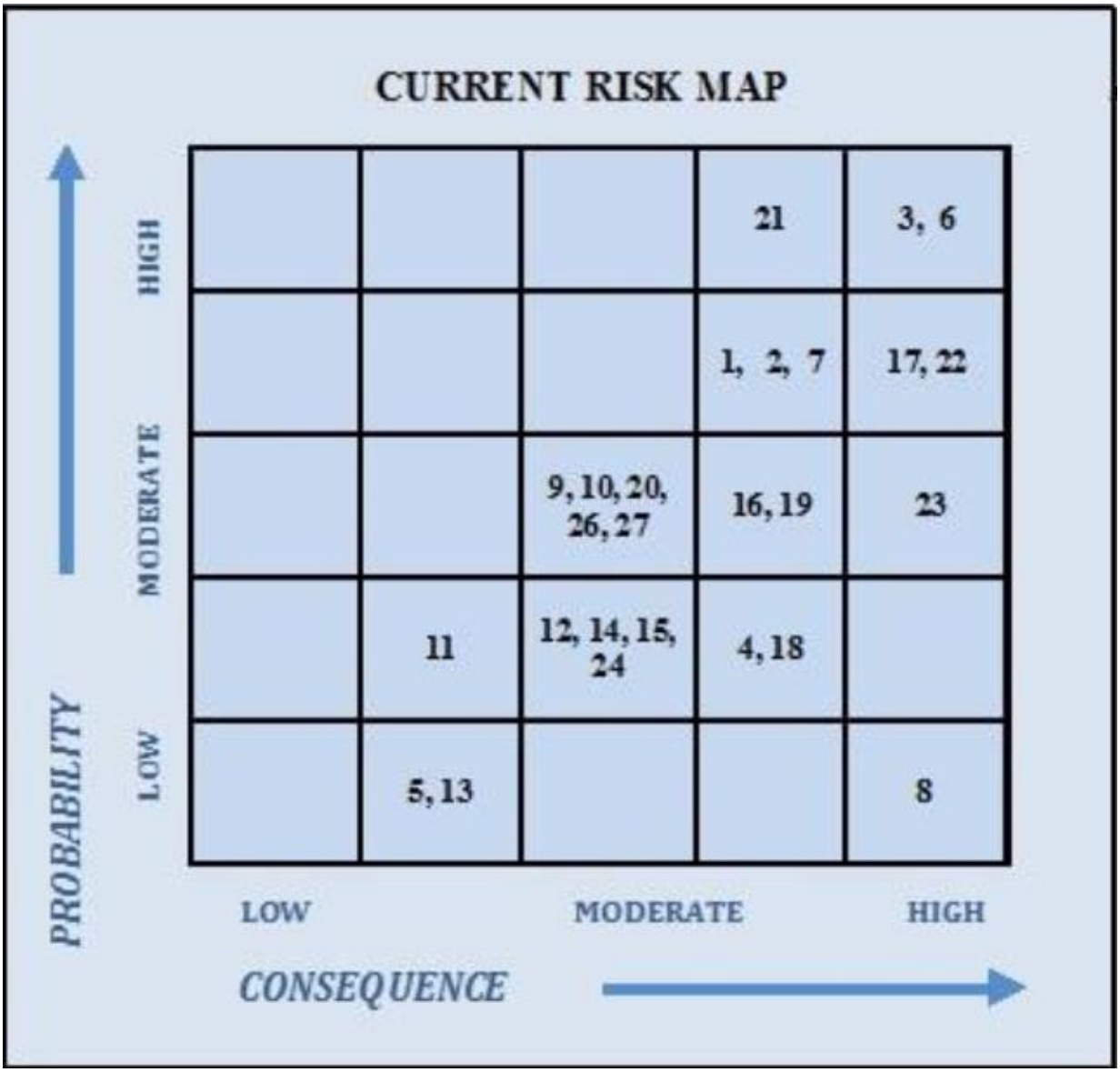
		Quarterly Video Conferences, provide forum for guest speakers from regulatory agencies to address update on regulations and answer questions, provide a classified briefing on threats to NASA export controlled technology, provide a forum for the Administrator to address Center Export Control Staff and answer questions	Control Representatives, other Center Export Control support staff, contractor personnel that support export compliance activities
Identity, Credential, and Access Management (ICAM) Identity SME/SETE	Bi-weekly	Provide identity related system development updates, receive feedback, and make changes to the tools before release.	Center identity subject matter experts and subject element technical experts.
ICAM Foreign National Identity SME/SETE	Bi-weekly	Provide foreign national related system development updates, receive feedback, and make changes to the tool before release.	Center foreign national subject matter experts and subject element technical experts.
ICAM User group	Bi-weekly	Primary communication channel to receive info on new releases/enhancements or reviews.	All ICAM users. (ICAM Center Subject Matter Experts, ICAM Subject Element Technical Experts from Centers, Mission Directorate and NEACC)
ICAM Working Group	Bi-weekly	Agency wide ICAM related items and issue working group.	Membership includes subject matter experts and subject element technical experts from each Center, Mission Directorate, and our applications center in Huntsville.
Physical Access Management (PAM) SME/SETE	Bi-weekly	Physical access management related release/enhancements, discussion of issues, feedback on center needs.	Physical access management subject matter experts and subject element technical experts.
NASA Consolidated Active Directory (NCAD), NASA Operational Messaging and Directory(NOMAD) CCB	Weekly	Discuss and vote on proposed change requests and any possible impacts.	NCAD Engineering, EUSO staff, ACES technical support
ICAM Identity	Bi-Weekly	Focus on identity creation. On-	ICAM Center Subject Matter

SME/SETE		boarding and off-boarding processes	Experts, ICAM Subject Element Technical Experts
MSFC PSD managed "Foreign Visit Escort Certification Course"	As required.	CISAs provide escorts training and education about intelligence collection techniques and other tactics that may be employed by foreign visitors.	PSD, IVC/FNAM managers, Center Escorts.
NASA Summer Internship Programs	Annually	(*Tailored CI Support*) CISAs vet FN (international) students and provide escorts training and education about intelligence collection techniques and other tactics that may be employed by foreign visitors.	PSD, IVC/FNAM managers, Event managers, Center Escorts.
NASA Robotics Mining Competition (KSC)	Annually	(*Tailored CI Support*) CISAs vet FN (international) students/participants and provide escorts training and education about intelligence collection techniques and other tactics that may be employed by foreign visitors.	PSD, IVC/FNAM managers, Event managers, Center Escorts
International Military Student Screening Program (SSC)	As required	(*Tailored CI Support*) CISAs vet FN (international) students attending the US Navy "NAVS/SCIATTS" program at SSC.	PSD, IVC/FNAM managers, and Event managers.
Space Studies Program (GRC)	Annually	(*Tailored CI Support*) CISAs vet FN (international) students/participants and provide escorts training and education about intelligence collection techniques and other tactics that may be employed by foreign visitors.	PSD, IVC/FNAM managers, Event Sponsors, Center Escorts
NASA Rover Challenge (MSFC)	Annually	(*Tailored CI Support*) CISAs vet FN (international) students/participants and provide escorts training and education about intelligence collection techniques and other tactics that may be employed by foreign visitors.	PSD, IVC/FNAM Managers, Event Sponsors, Escorts.
NASA Space Science and Technology Center	As required	(*Tailored CI Support*) CISAs vet FN (international) students/scientists/engineers and	PSD, IVC/FNAM Managers, NSSTC Managers, Sponsors, Escorts.

(MSFC)		provide escorts training and education about intelligence collection techniques and other tactics that may be employed by foreign visitors.	
Quantum Computing Laboratory Research Program (ARC)	As required	(*Tailored CI Support*) CISAs vet FN (international) participants/scientists/engineers and provide escorts training and education about intelligence collection techniques and other tactics that may be employed by foreign visitors.	PSD, IVC/FNAM Managers, QuAIL Managers, Escorts.
International Air Attaché Visits/Tours Program (JPL/KSC)	Annually/As required	(*Tailored CI Support*) CISAs vet FN (international) participants/air attachés and provide escorts training and education about intelligence collection techniques and other tactics that may be employed by foreign visitors.	PSD, IVC/FNAM Managers, Event Managers, Escorts.
NASA SOFIA Program	As required	(*Tailored CI Support*) CISAs vet FN (international) participants/scientists/engineers and provide escorts training and education about intelligence collection techniques and other tactics that may be employed by foreign visitors.	PSD, IVC/FNAM managers, SOFIA managers, Escorts.
CI Support to NASA HQ/Center FNAM Program	Routinely/As required	HQ/Center CI offices work closely with their respective PSD, IVC/FNAM managers on a day-to-day basis to vet FN/international visitors from a CI/CT perspective and coordinate concerns directly with HQ/Center managers and the US Intelligence Community.	HQ/Center PSD, IVC/FNAM managers, USIC.
CI Support to NASA FN Visitor Hosts/Escorts	Routinely/As required	HQ/Center CI offices provide CI education to NASA hosts/escorts who host/escort FN visitors from designated countries and Russia (as well as hosts/escorts of non-designated country visitors when warranted).	HQ/Centers Hosts/Escorts.

CI Support - LPR Employees/Visitors	Routinely/As required	(*Tailored CI Support*) HQ/Center CI offices vet LPR employees/visitors (that are born or citizens of a designated country) from a CI/CT perspective and coordinate concerns directly with HQ/Center managers and the US Intelligence Community.	HQ/Centers Managers and USIC.

Appendix F: Risk Map (Taken from 2014 Panel Report)



National Academy of
Public Administration ®

1600 K Street, N.W.
Suite 400
Washington, D.C. 20006
Phone: (202) 347-3190
Fax: (202) 223-0823
Website: www.napawash.org