WRITTEN STATEMENT

By

DICK THORNBURGH, PANEL CHAIR

NATIONAL ACADEMY OF PUBLIC ADMINISTRATION

BEFORE THE

HOUSE COMMITTEE ON APPROPRIATIONS

SUBCOMMITTEE ON COMMERCE, JUSTICE, SCIENCE, AND RELATED AGENCIES

TUESDAY, APRIL 8, 2014

Good morning Mr. Chairman and members of the Committee. Thank you for providing me with the opportunity to present the National Academy of Public Administration's assessment of NASA's Foreign National Access Management practices. As a Congressionally-chartered non-partisan and non-profit organization with nearly 800 distinguished Fellows, the Academy brings seasoned experts together to help public organizations address their most critical challenges. The Academy is proud to have been chosen by NASA to review how it meets those challenges. Not only has the Academy conducted a number of important studies for NASA in the recent past, but both organizations share a common lineage in the person of James Webb, the second NASA Administrator and founder of the Academy in 1967.

NASA's charter directs the agency to work cooperatively and share information with other nations while simultaneously safeguarding its classified and proprietary information and assets. This can prove to be a challenging task. On the one hand, the threat of cyber-attacks and espionage aimed at government agencies by hostile nation-states and foreign adversaries is growing. On the other hand, collaboration and cooperation between nations are hallmarks of modern scientific endeavors.

Over the last year, security incidents involving foreign nationals at NASA research centers have led to justifiable scrutiny by the NASA Administrator, the media and most particularly, this Committee. Recognizing these security challenges, NASA contracted with the Academy to conduct a review of its foreign national operations. How well NASA is able to balance their sometimes conflicting research demands, and what it might do to improve its processes for working with foreign nationals, were at the heart of this review.

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 Foreign National Access Management 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.

> Before I present the Panel's findings I would like to note that NASA provided complete cooperation for this review and that NASA interviewees 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. During this review, Academy staff interviewed over 150 individuals during visits to 5 NASA Centers, NASA Headquarters and several other Federal agencies. They also reviewed all relevant FNAM directives, reports and studies.

The Panel is sensitive to current Federal budget challenges and has worked to keep its recommendations within achievable budget limits although some may prove to be resource-intensive. The Panel believes that NASA can not only make mission and security improvements to existing foreign national access systems by following its recommendations but can also realize long-term potential savings by managing its foreign national efforts in a more efficient and effective manner. This testimony will represent the major findings of the Academy Panel's review that generally follow the overarching areas NASA asked the Academy to review.

Organizational and Functional Relationships

There is no systematic approach to FNAM at NASA; rather, there are individual (HQ) program requirements coupled with individual Center approaches. Simply put, there is no overall FNAM program, just separate FNAM processes – credentialing, export control, counterintelligence, IT access, etc. – that are viewed as a series of related tasks performed by independent organizations and individuals, and which often result in less than optimal outcomes.

When FNAM is viewed through these individual lenses, the judgments made about its efficacy are often subjective and incomplete. Evaluations focus on the various components without consideration given to the overall effect of these processes. When coupled with the lack of good program audit mechanisms, the chances for things going wrong rise significantly. This is particularly ironic, given that NASA is one of the most successful organizations in the world at practicing high-quality program management. The Panel has no doubt that any effort by the Agency to take a Program Management approach to FNAM would be successful.

FNAM Directives

An integral part of this review involved assessing the efficiency and effectiveness of the guidance provided by specific NASA publications pertaining to Foreign National Access Management (FNAM). In general, the Academy found that NASA Procedural Requirements (NPRs) and NASA Policy Directives (NPDs) were comprehensive, well-written, and easily accessible through NASA's online library. These documents provided answers to the "who, what, why, where, and when" questions, but did not adequately provide effective and practical guidance on "how" responsible individuals, officials, and entities were to perform their designated tasks. This was determined to be particularly true with processes that involved multiple individuals and organizations.

Through the interviews conducted at the Centers, it was clear that employees and contractors were aware of the existence of the FNAM publications, but those documents 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. In some cases, Centers have developed and published their own procedural requirements that were found to be more practical and user-friendly.

The Panel notes that uniformity and consistency in organizational performance by other federal agencies is directly correlated with the existence and routine use of agency-wide, clear, and concise direction and guidance. Most often, this guidance is disseminated through the publication of manuals and guidelines that provide simplified and practical instruction on the performance of specific tasks, as required by procedural and policy mandates. This observation was independently validated by NASA interviewees who noted the need for specific guidance on how to best perform certain FNAM functional requirements – that is − vetting, credentialing, sponsoring, escorting, and export control.

NASA states that compliance with each NPR and NPD is mandatory, and accountability for the aspects of each program and function is established. Despite these statements, the Academy found that there is little accountability for non-compliance when identified through specific incidents or periodic assessments. This validates the identified perception among NASA personnel that "mandatory compliance" means little, as there are few, if any, consequences for deliberate or inadvertent violations of the mandates. This combination of overly-broad directives combined with limited accountability has led to both varying processes and undesired outcomes.

NASA Decentralized Management

NASA needs to take steps to reduce the decentralized authority given to Centers for implementing FNAM and other largely procedural or enterprise-wide processes. NASA has a longstanding, highly decentralized organizational structure, with very independent field Centers. Allowing Centers great latitude to implement policies to fit their particular circumstances has the advantage of improving prospects for buy-in and creating policies and procedures which best fit local circumstances, but it can hamper enterprise solutions when such solutions are required. Different interpretations of NASA Procedural Requirements by individual Centers can result in widely varying FNAM performance among Centers.

If too much flexibility in largely procedural processes (which is what much of FNAM consists of) is coupled with a "stovepiped" organizational structure as mentioned above, then results become less predictable and often the opposite of what was intended. The benefits of tailoring and flexibility are outweighed by the inconsistency and often poor outcomes that result from this approach.

Tracking Foreign Nationals at NASA

Individuals requiring access to NASA facilities undergo vetting via an automated system designed to capture and store identity and credential data based on the visit type, residency and country affiliation. A requestor must submit a request for a visit via the **Id**entity **M**anagement and **A**ccount E**x**change (IdMAX) system which is an automated workflow tool used to process individuals for access to NASA facilities. IdMAX provides a record for identity confirmation and type of access (visitor, staff, contractor, foreign national), whether IT access is allowed and to what level. It is a single repository for anyone with access to NASA facilities or NASA data. The database asks a series of questions to determine level of access based on confidence and risk factors and is part of a larger program called Identity Credential and Access Management (ICAM).

The review found inconsistent application of and compliance with established policies, as well as broad interpretation of the NPRs regarding IdMAX. Centers have established different processes for the same activities, e.g. processing foreign nationals onto the facility and deciding who is allowed access to the systems.

Information Technology Security

A 2013 NASA IG Audit on Information Technology Governance stated that the NASA CIO has a restricted ability to standardize assets across the Agency to ensure that security policies are adhered to. The OCIO also has very limited capabilities for monitoring the Agency's mission networks and has to instead rely on self-reporting of vulnerabilities by the mission IT staffs. These limitations are further compounded by the fact that NASA does not have a complete inventory of IT assets. The Academy's research and findings in these respects are consistent with the IG report.

NASA systems are decentralized and the responsibility for management and security is delegated to the Centers. Center CIOs and system owners have considerable autonomy in managing their systems. System owners determine access controls and have the ability to add networks or connect to external networks. Most Center CIOs have the ability to monitor the "health" of their networks locally, but no authority to require that system owners allow monitoring by the Center or the Security Operations Center (SOC). Most of them noted that they have no ability to prevent mission managers from establishing stand-alone systems or adding back end connections to the network.

NASA has a culture of information sharing and Agency information systems were designed to facilitate such sharing as opposed to identifying, monitoring or preventing potential threats. A 2010 NASA memorandum highlighted the state of NASA systems, and the impacts of unauthorized access to Agency systems, to include *"loss of productivity, theft of intellectual property (data exfiltration), and public embarrassment."* A NASA white paper from that same year outlined the state of NASA's compromised environment, providing details of the threats the Agency faced, the vulnerabilities that were being exploited and detailed examples of recent incidents.

Due to the fact that the NASA systems lack the necessary controls to protect information, allow foreign nationals access to the networks, and allow remote access, the Panel concludes that the NASA networks are compromised. Publicly available reports on systemic data breaches across the country, NASA's own internal reports, and briefings given to Academy staff leave little doubt that information contained on the NASA IT systems is compromised.

Counterintelligence Awareness and Education Programs

NASA directives state that the purpose of the counterintelligence and counterterrorism (CI/CT) program *"is to detect, deter, and neutralize potential threats posed by foreign intelligence services (FIS), other foreign entities, and acts of terrorism to include trusted insiders who would engage in activities on behalf of an FIS or terrorist entity."* When NASA's CI Program was created, no additional personnel were hired. Instead, CI responsibilities were given to Center security personnel as ancillary duties. A 2000 study of NASA's counterintelligence capabilities recommended that the CI personnel be assigned to CI matters on a full-time basis, and be responsible to both Center management and HQ. NASA assigned CISAs to work only CI/CT matters and then centralized the CI/CT program under the Director of the CI/CT Division at HQ.

The Panel found that the current number of personnel assigned to the CI/CT Program is inadequate to formulate, manage, and perform effective CI Awareness and Education programs and that Center-based CI Special Agents (CISAs) would function more effectively if placed under Center management with close HQ oversight. The Panel also found that CI awareness briefings do not seem to be a priority and that CI awareness and education at the Centers and at HQ varies greatly, with some being ineffective.

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. The Academy found that most CI Special Agents appear to be very conscientious in contacting travelers to Designated Countries and high-threat areas, and in providing updated travel briefings. Some Centers send significantly more foreign travelers to Designated and high-threat countries than others, and the Special Agents in these high-travel Centers are especially diligent in their attempts to brief all of their frequent travelers.

Procedures for Hosting and Escorting Foreign Nationals

Hosting of visitors to NASA facilities, including foreign nationals, can encompass all phases of Foreign National Access Management (FNAM) – from initial identification of foreign visitors through termination of their physical or remote access to NASA assets. This can also involve policies, procedures, and processes pertaining to foreign national vetting, badging, escorting, accessing facilities and information technology systems, export control issues, monitoring, awareness and training, as well as the interrelationships of the NASA HQ and Center organizations.

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. 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.

Foreign National Access Management (FNAM) procedures, particularly for those 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. Integrated Functional Reviews and CI/CT Evaluations which NASA conducts do not specifically address the performance of the tasks pertaining to hosting/sponsoring and escorting foreign nationals and the required briefings of sponsors and escorts of foreign nationals have not adequately conveyed the risk that an individual might pose to NASA assets.

Export Control

NASA's export policy directive clearly states that it "*is NASA policy to ensure that exports and transfers of commodities, technical data, or software to foreign persons are carried out in accordance with the United States export control laws and regulations, and Administration and NASA policy.*" 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. The training provided to Center staff members who need to be aware of export control issues is Center-centric and widely-varied. Some Centers have mandated training for all staff on an annual basis. Others take a more *laissez-faire* approach with training either being optional or, if mandatory, provides no sanctions against those who fail to take the training.

These *laissez-faire* approaches tend to create misunderstandings and even a degree of mistrust and hostility between the various parties. Academy staff heard numerous complaints from researchers about Center Export Administrators (CEAs) and their "unnecessarily bureaucratic" and "time-consuming" reviews and conversely, heard complaints from CEAs about "unreasonable" demands for turning-around documents which always seem to be submitted for review at the last minute. Such complaints indicate a lack of communication about both time frames and rationales for these types of security measures. In summary, the Panel Export control training requirements are inconsistent; the training is confusing and inadequate; and the rationale for such training is often poorly understood.

Monitoring FNAM Compliance and Performance

NASA needs more robust mechanisms for ensuring that FNAM policy requirements are being met by field Centers. There have been recent improvements by NASA HQ in auditing and assessing field Center FNAM efforts but more needs to be done. Absent an improved system of oversight, the Agency will remain uncertain about how well FNAM is being conducted. There are a number of time-tested approaches to this but one which needs to be considered is the use of cross-functional teams to review Center FNAM operations. Such teams could review the individual program compliance metrics (e.g., export control, credentialing, etc.) as well as the overall performance and outcomes of FNAM at the Center. Team membership should include not only HQ program specialists but also FNAM staff from other Centers to both provide a field perspective and to propagate the cross-fertilization of ideas.

As opposed to doing the organizational-specific compliance audits as is the practice today, the teams' reviews should result in comprehensive Center-specific assessments in which all physical, technological and informational assets are identified; actual and potential threats to those assets evaluated; risks assessed; protective strategies developed; and resource requirements prioritized.

Asset Protection

The task of protecting NASA's assets – its facilities, personnel, technologies, and information – is a multi-dimensional responsibility involving every NASA civil servant, contractor, and organization, as well as the support and assistance of other agencies. The successful performance of this task is dependent on completion of a number of interrelated functions – identification of assets requiring protection, accurate intelligence regarding threats, design and implementation of protective strategies, education and awareness of NASA personnel, and continuous evaluation to ensure threats are countered commensurate with their importance. This requires a comprehensive approach to risk management, employing the best practices available.

During this study, the Academy observed the following regarding NASA's asset protection efforts:

- Centers differ in their efforts to identify assets that require protection, with responsibility placed on several different components.
- Threats have not been adequately conveyed to Center personnel.
- Extensive instructional/training material available through the FBI, Department of Energy (DOE), Office of the National Counterintelligence Executive (NCIX), and other Intelligence Community (IC) agencies has not been utilized to educate NASA staff on the threats posed by insiders, hostile intelligence services, terrorism, and economic espionage.
- Specific intelligence regarding threats posed by foreign nationals and insiders to specific NASA assets is available from IC agencies, but has been inconsistently utilized to educate NASA personnel.
- Detailed policies, procedures, and instructions regarding comprehensive approaches to asset protection have been implemented by other agencies, particularly DOE, and should be reviewed for possible utilization by NASA.
- Independent and Management Assessment and Evaluations, employed by IC agencies, should be regularly utilized to determine the effectiveness of NASA's asset protection efforts, gaps in those procedures, and assurance that proper resources are committed commensurate with the risk.

NASA needs to reconsider how it assesses and protects its information and security assets in the field. While this review has focused on FNAM, the Panel believes that a broader approach to asset protection and oversight is needed. NASA facilities, personnel, technologies, and information are highly regarded and of great interest to the world. That interest extends to some countries, governments, organizations, and individuals whose intent is to compromise those facilities, co-opt the personnel, and steal those technologies and information. While NASA currently conducts annual threat assessments at every Center by the Protective Services office, counterintelligence special agents, and the CIO, those assessments address only the areas of responsibility of those individual offices. They are not comprehensive, Center-specific assessments that consider all the elements necessary to fully protect NASA's assets.

The Panel believes NASA needs 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 technical data and proprietary information, not simply the data potentially exposed to foreign nationals and to also compile threat assessments from the various elements into comprehensive Center and agency threat/risk assessments. These assessments could be incorporated into NASA's risk management process. By establishing a mechanism for comprehensive, Center-specific assessments NASA could identify and prioritize vulnerable assets, assess protective strategies, allocate resources commensurate with the risk, and evaluate the overall asset protection efforts.

NASA Internal Controls and Risk Management

NASA needs to reconsider how it assesses and protects its information and security assets in the field. The NASA Management System Working Group (MSWG) serves "as the Community of Practice (COP) for NASA internal controls activities and the effective integration of internal controls into any agency-wide Integrated Management System (IMS)." The MSWG scope covers NASA Headquarters, NASA Centers, and their associated facilities. This charter is consistent with the broad scope intended by OMB Circular A-123. Unlike many federal agencies that implement internal controls with an overly strong focus on financial reporting. MSWG is a newly-revised organization under the direction of a new Associate Administrator.

While responsibility for internal controls over financial reporting is placed under the NASA Chief Financial Officer, overall responsibility for NASA-wide internal controls – and providing direction to the MSWG – is placed under the Director, Office of Internal Controls and Management Systems, who in turn reports to the Associate Administrator for Mission Support. This management structure clearly signals NASA's recognition that internal controls apply universally across all areas of the agency, and is not focused exclusively on financial reporting.

While NASA's intent is to establish an internal controls management framework across all organizational elements, the effective implementation of the policy outlined is not consistent. A Senior Assessment Team (SAT) oversees the internal controls program and has as members representatives from all program and functional areas of NASA. However, the SAT is able to assess, prioritize and correct control deficiencies only to the degree such deficiencies are brought to the SAT's attention. Unfortunately, there are management processes operating at the Center level that identify problems and risks, but that are disconnected from the internal controls process.

NASA's Surveys, Audits and Reviews (SAR) Policy generates insights at the Center-level on various risks and problems. However, the only formal connection between this set of processes and the internal controls program is that Center Directors submit their Certification Statements to HQ to be included in the Agency's annual Assurance Statement. To the degree that the [SAR] program identifies risks associated with internal operations and processes, there should be a communications path to ensure such risks and control deficiencies inform the internal controls program. Moreover, all control deficiencies identified at the Center level are not currently required to be reported to Headquarters. As a result, there is no ability of the SAT to independently assess the degree of completeness of information forwarded to the SAT by the Center. Meaningful transparency would allow the SAT complete access to internal controls findings at the Center level.

The Panel notes that NASA's annual Statement of Assurance (SoA) rolls up/includes risks that are obtained from the Centers and NASA policies make it clear that internal controls are the responsibility of the Center Directors and other appropriate officials who also are required to perform self-assessments and submit Certification Statements. However, the Panel believes that the current process is not sufficient and that an oversight entity is needed by NASA to focus on the following goals and objectives:

- Develop a multi-disciplinary template for use by Center personnel to periodically identify assets to be protected, internal and external threats based on self-assessments and intelligence received, resource and/or technological enhancements needed, and deficiencies identified and/or improvements required.
- Collate the comprehensive Center risk assessments into an agency-wide risk assessment to be provided to executive management for determining resource allocation, budgetary requests, and organizational performance assessments.
- Center and agency risk assessments should be provided to those entities having internal control responsibilities, to include the CFO and MSWG.
- Enhance liaison with Intelligence Community (IC) agencies to disseminate and vet Center and agency risk assessments, obtain current intelligence on targeting of NASA assets by individuals, organizations, or governments, leverage successful protective strategies developed by those agencies, and utilize their training and awareness materials and resources to educate NASA civil servants and contractors.

- Establish an Independent Assessment/Inspection team to periodically assess and evaluate each Center's organizational and functional performance in all facets of asset protection, to include FNAM, physical security, IT security, export control, training and awareness, and liaison. Particular emphasis should be placed on evaluating organizational interactions and relationships, with input from Center management and affected personnel.

The Panel believes that establishing a mechanism for comprehensive, Center-specific assessments and creating an oversight entity to manage this process would allow NASA to fully integrate both its HQ and Center internal controls and risk management efforts into a comprehensive and cohesive effort.

Potential Organizational Changes

There are a several organizational changes NASA can make to strengthen FNAM. The Panel believes that Counterintelligence Staff in the field would function more successfully if they were integrated into the field Protective Services staff under the ultimate supervision of the Center Director. Although plausible arguments can be made to keep the CI staff under HQ management, observations by Academy staff during field Center visits, as well as the CI/CT assessment of 2000, led to the conclusion that the special agents would be more integrated into overall operations, and consequently more successful, if put under Center management. The danger of having them diverted to non-CI tasks as has taken place in the past when they were under Center management, can be mitigated by having clear policies forbidding same and strong audit reviews to make sure it is not happening.

The Panel also thinks the time is appropriate for an elevation of the organization with the primary responsibility for Foreign National Access Management – Protective Services in NASA Headquarters – to be moved 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.

Finally, certain key FNAM-related jobs in the field, specifically the Chiefs of the Office of Protective Services, Center Export Administrators, and Counterintelligence Special Agents should have formal, recognized relationships with their HQ counterparts. Forging a strong linkage (a "dotted-line" organizational relationship) between the HQ and field entities can only strengthen FNAM. Currently, Center OPS Chief selections and evaluations require the endorsement of the HQ Assistant Administrator for OPS. Although there are consultations regarding selections, Academy staff could not find evidence that HQ endorses Center OPS Chiefs' evaluations.

The NASA CIO is currently the supervisor of Center CIOs but there are two observations the Panel makes about this: first, some Center CIOs interviewed by Academy staff were unaware of this reporting responsibility; and, second, the Panel believes mission CIOs should also require the NASA CIO's endorsement prior to their selection and annual evaluation. That currently is not the practice at NASA. The Panel believes that forging a strong link between these line and staff positions while still maintaining a strong field-based approach will help ensure that asset protection is well done and remains a priority.

Competition between Field Centers

Unnecessary competition between Centers is counterproductive. Competition can potentially hamper non-mission activities that often require a more structured, consistent approach, and most particularly, the sharing of best practices. Having Centers struggle to solve problems that other Centers already resolved, which the Academy staff observed during their Center visits, is a waste of time and money and jeopardizes the success of the program. When it comes to FNAM, Center competition does not "improve the breed." It actually hurts in two ways: Centers with solutions might be disinclined to assist "competitors" and Centers experiencing problems might be concerned about exposing weaknesses in their operations.

An additional consideration is the need for NASA to approach its current budget situation in an organizationally united fashion. Competition between Centers is anathema to this requirement. NASA budget constraints – "flat is the new up" – require a mission approach that drives Centers to work collaboratively with each other and HQ, to ensure that scarce mission-critical resources are not squandered by unnecessary redundancy and waste.

NASA Culture

Any discussion of Foreign National Access Management problems and potential solutions must take into account NASA culture which plays an important role in every aspect of NASA operations. NASA is seen as a desirable place to work with a highly-educated, talented and committed, but rapidly-aging, workforce. In 2013, it was ranked "Best Place to Work in Government" in an annual poll. The Agency has an important, high-profile mission and the NASA "brand" is recognized and admired throughout the world. NASA culture plays an important role in creating these attitudes and perceptions.

NASA research is done largely in a collegial atmosphere with the grounds on each Center being referred to as a "campus." This fosters the sharing of information, an essential element in research, but can create tension between the need to collaborate and the need to protect classified or otherwise sensitive information. There is also a tendency for some staff to find a "work-around" for procedures and policies they do not agree with or believe to be erroneous, including some FNAM requirements. NASA also often uses an informal (i.e., non-hierarchical) approach to management of people and processes. Directives, and orders, can be seen more as “guidance” as opposed to mandatory policy and procedural requirements that must be adhered to. This can lead to communications breakdowns and negative outcomes.

NASA leaders shared the concern with Academy staff that after fixing a problem, the Agency has a tendency to lapse back into old habits once the spotlight is off the area under review, in this case, FNAM. A number of NASA leaders also noted that the Agency tends not to hold individuals accountable even when they make serious, preventable errors. Whenever an example of such an error was mentioned during the interviews, Academy staff would follow-up with: *what happened to those responsible for the error?* In almost every instance, the answer was either “nothing” or “I don’t know.” The belief that individuals are not held accountable for ignoring or deliberately failing to comply with FNAM requirements is widespread and includes both managers and rank-and-file employees.

If there are no consequences for ignoring or significantly deviating from a policy requirement or directive, then the chance of the policy or directive being implemented as intended decline dramatically. An important element in changing this attitude and driving compliance is the certainty that processes and outcomes will be reviewed by external entities. This is not to suggest a harsh or unforgiving approach to discipline; the goal is not punishment but reinforcement of behavioral norms.

Panel Recommendations

The Panel made 27 recommendations to NASA as to how it can improve its Foreign National Access Management in its final report which can be summarized into the following six headings:

1. **Manage FNAM as a Program.** The Panel proposed a number of steps for NASA to take which would begin to coordinate efforts and secure better results including realignment of both field and Headquarters organizational elements, strengthening the oversight capabilities of headquarters, and, improving training by developing comprehensive, integrated curriculums and lesson plans.
2. **Reduce the flexibility given to Centers to interpret FNAM requirements.** The Panel recommended that NASA Headquarters write a comprehensive and detailed FNAM operating manual covering all functional aspects of the program. Currently, FNAM directives can be found in several different publications, each with their own Headquarters and field constituencies. Headquarters staff should work in consultation with knowledgeable field staff to create this manual.
3. **Determine critical assets and build mechanisms to protect them.** The Panel envisions the creation of an Asset Protection Oversight Board which would use the results of the Independent Review Teams assessments of individual program compliance metrics as

well as overall performance and outcomes of FNAM and the adequacy of the comprehensive threat/risk assessment at each Center.

4. **Correct longstanding information technology security issues.** The Panel believes NASA needs to identify and protect sensitive, proprietary information in a manner that does not prevent system owners from meeting their mission needs. Among the specific recommendations in this area are for NASA to establish clear, specific, and mandatory requirements for all Centers to follow regarding remote access of their information technology systems and that the NASA Chief Information Officer be given more control over IT operations in field Centers.

5. **Work to change several aspects of NASA culture.** Included in this are the recommendations to reduce unnecessary competition between field centers, ensure that accountability for conforming to FNAM requirements is established, and finally, to guard against the organizational tendency to revert back to prior lax habits once a problem area has been addressed.

6. **Communicate the importance of these FNAM 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 Foreign National Access Management program that enhances cooperation while safeguarding information.

In closing, let me note that the Academy was pleased and honored to work with NASA and the Committee on this review and to present this testimony today. I believe that we have provided NASA with a good template for building a robust and effective Foreign National Access Management program and that the Agency has the right leadership and commitment to make that happen. With the Committee's support and oversight, I am certain this program will provide NASA with the foreign talent it needs to fulfill its mission while capably safeguarding sensitive information.

Thank you for providing me this opportunity to share these views with you.