SECURING FEDERAL FACILITIES: AN EXAMINATION OF FPS PROGRESS IN IMPROVING OVERSIGHT AND ASSESSING RISK

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

JULY 24, 2012

Serial No. 112–108

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.gpo.gov/fdsys/

U.S. GOVERNMENT PRINTING OFFICE

80–850 PDF WASHINGTON : 2013

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

PETER T. KING, New York, *Chairman*

LAMAR SMITH, Texas
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
MICHAEL T. MCCAUL, Texas
GUS M. BILIRAKIS, Florida
PAUL C. BROUN, Georgia
CANDICE S. MILLER, Michigan
TIM WALBERG, Michigan
CHIP CRAVAACK, Minnesota
JOE WALSH, Illinois
PATRICK MEEHAN, Pennsylvania
BEN QUAYLE, Arizona
SCOTT RIGELL, Virginia
BILLY LONG, Missouri
JEFF DUNCAN, South Carolina
TOM MARINO, Pennsylvania
BLAKE FARENTHOLD, Texas
ROBERT L. TURNER, New York

BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
SHEILA JACKSON LEE, Texas
HENRY CUELLAR, Texas
YVETTE D. CLARKE, New York
LAURA RICHARDSON, California
DANNY K. DAVIS, Illinois
BRIAN HIGGINS, New York
CEDRIC L. RICHMOND, Louisiana
HANSEN CLARKE, Michigan
WILLIAM R. KEATING, Massachusetts
KATHLEEN C. HOCHUL, New York
JANICE HAHN, California
RON BARBER, Arizona

MICHAEL J. RUSSELL, *Staff Director/Chief Counsel*
KERRY ANN WATKINS, *Senior Policy Director*
MICHAEL S. TWINCHEK, *Chief Clerk*
I. LANIER AVANT, *Minority Staff Director*

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES

DANIEL E. LUNGREN, California, *Chairman*

MICHAEL T. MCCAUL, Texas
TIM WALBERG, Michigan, *Vice Chair*
PATRICK MEEHAN, Pennsylvania
BILLY LONG, Missouri
TOM MARINO, Pennsylvania
PETER T. KING, New York *(Ex Officio)*

YVETTE D. CLARKE, New York
LAURA RICHARDSON, California
CEDRIC L. RICHMOND, Louisiana
WILLIAM R. KEATING, Massachusetts
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

COLEY C. O'BRIEN, *Staff Director*
ZACHARY D. HARRIS, *Subcommittee Clerk*
CHRIS SCHEPIS, *Minority Senior Professional Staff Member*

CONTENTS

SECURING FEDERAL FACILITIES: AN EXAMINATION OF FPS PROGRESS IN IMPROVING OVERSIGHT AND ASSESSING RISK

Tuesday, July 24, 2012

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES,
Washington, DC.

The subcommittee met, pursuant to call, at 10:09 a.m., in Room 311, Cannon House Office Building, Hon. Daniel E. Lungren [Chairman of the subcommittee] presiding.

Present: Representatives Lungren, Walberg, Clarke, Richmond, and Keating.

Mr. LUNGREN. The Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies will come to order. The subcommittee is meeting today to examine the Federal Protective Service and the possible need for reform.

Ms. Clarke will be here shortly, and so I am just going to give my opening statement and when she arrives she will be able to give her opening statement.

Thank you very much for being here, all three of our witnesses. This is an important hearing.

The Federal Protective Service is a vital part of the Department of Homeland Security. It is the largest operational component within the National Protection and Programs Directorate.

The FPS mission is to protect over 9,000 Government buildings and their 1.4 million occupants, which are essential to the day-to-day operations of the Federal Government. Recent incidents at Federal facilities such as the failed improvised explosive device, as well as the bombing of Oklahoma City's Murrah Federal Building in 1995, remind us the Federal facilities remain attractive terrorist targets.

This subcommittee has conducted rigorous oversight over the Federal Protective Service this Congress. Last July we held a hearing which identified some of the perennial problems plaguing the FPS.

In that hearing we discussed failures of contract guard oversight and their training program, including the egregious mishandling of an IED in Detroit. We also discussed the failed development of FPS's risk management program, known as RAMP, which cost the Federal Government $35 million over 4 years. I am hopeful and

cautiously optimistic that these problems represent the low-water mark for FPS.

Since 2008 GAO has made 32 recommendations to improve FPS security vulnerabilities and other operational problems, five of which have been implemented and 20 which are in the process of implementation.

From the outset I do want to commend Director Patterson for his leadership. I believe the recent successes in implementing GAO recommendations are in part the result of improved dialogue and outreach with the private sector as well as the efforts of FPS's own workforce.

I think this dialogue is extremely important as FPS works to address the remaining GAO recommendations, especially in its two core areas of responsibility: First, its ability to conduct risk assessments of Federal buildings; and second, to provide necessary oversight and training for its contract guard force.

Regarding the first responsibility, FPS began operational testing this last spring for a new risk assessment tool, known as the modified infrastructure survey tool, or MIST, which was developed in partnership with the Argonne National Laboratory. MIST is intended to be an interim tool that FPS inspectors use to conduct vulnerability assessments in the aftermath of the RAMP failure.

I understand, am informed that there is a disagreement between FPS and GAO with regard to the limitations and benefits of MIST and I look forward to hearing from our witnesses regarding these differences. I am aware of some of the limitations identified by GAO that MIST does not account for consequence information and therefore does not provide FPS the comprehensive ability to manage risk. I also understand GAO has concerns that MIST is neither compliant with the National infrastructure protection plan framework nor compliant with standards developed by the Interagency Security Committee.

I think these are very legitimate questions raised by GAO and important standards FPS should meet when it develops a longer-term solution. Nonetheless, I do consider MIST development a step in the right direction for an agency that has taken a series of steps in the wrong direction over the last decade.

FPS has always stated that MIST is intended to serve as an interim tool until a longer-term solution is developed. However, FPS has never stated what the longer-term solution will be. So I look forward to hearing from Director Patterson on his vision for MIST's future as a risk management tool.

I also look forward to learning about what FPS is doing to address GAO's findings about unnecessary duplication of risk assessments by several FPS customers who in some instances have expressed dissatisfaction with FPS's assessments—for instance, the IRS, FEMA, and EPA.

Providing oversight and training of the contract guard program is also a critical responsibility of FPS. At last summer's hearing Director Patterson stated that he was looking at different ways that FPS may be able to improve delivery of X-ray and magnetometer training.

I look forward to hearing more about how these ideas have developed since last year. I also understand there has been outreach to

the private sector regarding better training options and I commend you for those efforts.

Finally, FPS has undergone significant transition since joining the Department of Homeland Security. After initially being placed under ICE, after the creation of DHS, FPS moved to NPPD in 2010, and last summer NPPD notified the committee that it was once again considering reorganizing the directorate. Is reorganization being contemplated, and if so, how will this impact FPS?

I want to thank all of our witnesses for being here this morning, and I look forward to your testimony on the progress made by the FPS in securing our Nation's Federal facilities.

[The statement of Chairman Lungren follows:]

STATEMENT OF CHAIRMAN DANIEL E. LUNGREN

JULY 24, 2012

The Federal Protective Service (FPS) is a vital part of the Department of Homeland Security and is the largest operational component within the National Protection and Programs Directorate (NPPD). Its mission to protect some 9,000 Government buildings and its 1.4 million occupants is essential for the Federal Government to continue day-to-day operations. Recent incidents at Federal facilities such as the failed IED attempt in Detroit, and the bombing of Oklahoma City's Murrah Federal Building in 1995, remind us that Federal facilities remain significant symbolic targets for terrorists.

This subcommittee has conducted rigorous oversight over the Federal Protective Service this Congress. Last July we held a hearing which identified some of the perennial problems plaguing the FPS. In that hearing we discussed failures of contract guard oversight and training, including the egregious mishandling of an attempted Improvised Explosive Devise in Detroit, and the failed development of a risk management program known as RAMP, which after 5 years of development, cost the Federal Government somewhere between $35–57 million with little to show for. I am hopeful that these incidents represent the low-water mark for FPS, and I am cautiously optimistic about FPS's future.

Last July the GAO had issued a total of 28 recommendations for FPS to address, yet at the time none were implemented. Today, I am encouraged to note that while GAO has recommended 32 recommendations, to date, 5 have been implemented and 20 are in the process of implementation. This represents significant progress.

From the outset, I want to commend Director Patterson for his leadership and the agency's recent successes. These successes, I believe are in part the result of improved dialogue and substantial outreach with private-sector partners as well FPS's own workforce. I think this dialogue is extremely important as FPS works to address important recommendations made by the Government Accountability Office, especially as it works to improve two of its core areas of responsibility: (1) Its ability to conduct risk assessments of Federal buildings; and (2) provide necessary oversight and training for its Contract Guard Program.

Regarding this first responsibility, FPS began operational testing this last spring for a new risk assessment tool, known as the Modified Infrastructure Survey Tool or MIST, which was developed in partnership with the Argonne National Laboratory. MIST is intended to be an interim tool FPS inspectors use to conduct facility security assessments, in the aftermath of RAMP's failure.

I understand there is some pretty substantial disagreement between FPS and GAO with regard to the limitations and benefits of MIST and I look forward to hearing from our witnesses regarding these differences. I am aware of some of the limitations identified by GAO, such as that MIST does not account for "consequence" information, and therefore does not provide FPS the comprehensive ability to manage risk. I also understand GAO has concerns that MIST is neither compliant with the National Infrastructure Protection Plan framework nor compliant with standards developed by the Interagency Security Committee. I think these are very legitimate questions raised by GAO, and are important standards FPS should meet when it develops a longer-term solution.

Nonetheless, I consider MIST's development a step in the right direction for an agency that has taken a series of steps in the wrong direction over the last decade. FPS has always stated that MIST is intended to serve as an interim tool until a longer-term solution is developed. However, FPS has never stated what the longer-

term solution will be. I look forward to hearing from Director Patterson on his vision for MIST's future as a risk management tool. I also look forward to learning about what FPS is doing to address GAO's finding about unnecessary duplication of risk assessments by several FPS customers, who in some instances, are dissatisfied by assessments provided by FPS.

Providing oversight and training of the contract guard program is also a critical responsibility of FPS. At last summer's hearing Director Patterson stated that he was looking at different ways FPS may be able to improve delivery of X-ray and magnetometer training. I look forward to hearing more about how these ideas have developed since last year. I understand there has been significant outreach with the private sector that may be able to better deliver training, and I commend you for putting an emphasis on training in your tenure at FPS.

Finally, FPS has undergone significant transition since joining the Department of Homeland Security. After initially being placed under ICE after the creation of DHS, FPS moved to NPPD in 2010. Last summer, NPPD notified the committee that it was once again considering reorganizing the agency which FPS was assigned. However, since last summer, the Department has been silent on its plans to reorganize NPPD, so I am very much looking forward to hearing from Director Patterson on his thoughts on reorganization, and if we can expect any more information on this soon.

I want to thank all of our witnesses for being here this morning and look forward to their testimony on progress made by the FPS securing our Nation's Federal facilities. I now recognize the gentle lady from New York, the Ranking Member of this subcommittee, Ms. Clarke, for her opening statement.

Mr. LUNGREN. I now have the pleasure of recognizing the gentle lady from New York, the Ranking Member of the subcommittee, Ms. Clarke, for her opening statement.

Ms. CLARKE. Thank you, Mr. Chairman, and thank you for holding this hearing today. Today's hearing will allow the subcommittee to hear from witnesses about the Federal Protective Service's progress in improving its ability to provide adequate protection to the Federal Government's more than 9,000 facilities.

Given the numerous studies that FPS has undertaken by the Government Accountability Office and the multiple hearings held by this committee, the subcommittee is interested in learning about the actions FPS has taken to upgrade its ability to conduct facility security assessments, better manage its contract guard staff, and to enhance funding for its operations. We need a more clear explanation of the implementation and utility of the modern infrastructure survey tool, or MIST, and how it compares, hopefully surpasses, the failed risk assessment and management program, or RAMP.

The subcommittee must be assured that after investing approximately $35 million RAMP without yielding any demonstrable outcomes FPS is indeed expending its resources effectively and scaling up MIST. We need assurances that MIST is working as an interim solution, and we need to know what FPS's long-term strategy to replace RAMP. Also, as the designated leader of the Federal Government facilities sector FPS has an important role to play in assuring that the Federal critical infrastructure both secure—that the—excuse me—the Federal critical infrastructure is both secure and resilient in the event of a catastrophic occurrence.

In August GAO will issue a report at Ranking Member Thompson's request that evaluates the Department's activities regarding the Government facilities sector with a particular emphasis on FPS's role as the designated sector leader. I look forward to the release of that report and hope that we are able to revisit this subject at that time.

Finally, Mr. Chairman, I am concerned that FPS is forced to bear the cost of developing and implementing a program capable of completing security assessments of Federal buildings. It seems to me that as the landlord for most Federal buildings, the General Services Administration benefits from these security assessments. I look forward to hearing from our witnesses today about the role of GSA in sharing the cost of the assessment program.

Having said that, thank you, Mr. Chairman, and I yield back.

[The statement of Ranking Member Clarke follows:]

STATEMENT OF RANKING MEMBER YVETTE D. CLARKE

JULY 26, 2012

Mr. Chairman, thank you for holding this hearing to discuss developments in the Domestic Nuclear Detection Office Strategy, and the Global Nuclear Detection Architecture.

It has been said before, the enormous devastation that would result if terrorists use a nuclear weapon or nuclear materials successfully, requires us to do all we can to prevent them from entering or moving through the United States.

This subcommittee, in its oversight capacity, has held hearings starting in 2005, and continuing through 2012, regarding the development and implementation of the GNDA and in the decision-making process that involves costly investments in it.

The overarching issues include the balance between investment in near-term and long-term solutions for architecture gaps, the degree and efficiency of Federal agency coordination, the mechanism for setting agency investment priorities in the architecture, and the efforts DNDO has undertaken to retain institutional knowledge regarding this sustained effort.

In the policy and strategy documents of the GNDA, DNDO is responsible for developing the global strategy for nuclear detection, and each Federal agency that has a role in combating nuclear smuggling is responsible for implementing its own programs. DNDO identified 73 Federal programs, which are primarily funded by DOD, DOE, and DRS that engage in radiological and nuclear detection activities.

With the publication of an overall DNDO strategy document and the release of the Global Nuclear Detection Architecture and implementation plan, Congress will have a better idea of how to judge the DNDO's policy, strategy operations, tactics, and implementation.

But we need to know more about their R&D activities, their resource requests, and their asset allocations. And I know that I might sound like a broken record before the day is through, but from the very start of the ASP program which was officially cancelled just 10 days ago, July 16, DNDO seemed to push for acquisition decisions well before the technology had demonstrated that it could live up to its promise.

On July 14, 2006, Secretary of Homeland Security Michael Chertoff and the then-Director of DNDO, Mr. Oxford, one of our witnesses today, announced contract awards to three companies worth an estimated $1.2 billion to develop ASPs, including the Raytheon Company from Massachusetts, the Thermo Electron Company from Santa Fe, New Mexico, and Canberra Industries from Connecticut. Both Secretary Chertoff and Oxford held a press conference to announce the billion-dollar contract awards just a few months after highly critical reviews of the ASPs' abilities by the GAO and the National Institute of Standards and Technology (NIST).

I hope we don't see that kind of decision making again in DNDO.

Within DNDO, policy and strategy have historically not been adequately translated into operations, tactics, and implementation. Overlapping missions, especially in the field of nuclear detection, worsen this.

Since 2009, DNDO has made important changes under Secretary Napolitano, and made especially good progress in nuclear forensics. And I hope that our Congressional oversight has had an effect, a positive one, in bringing to light decisions that cost the taxpayers a lot of money, with little to show.

In 2010, the Science and Technology (S&T) Directorate requested $109.000 million for the Transformational Research and Development Radiological and Nuclear Division. This research was to be transferred from DNDO to the S&T Directorate,[1] and the Democratic committee Members supported the transition of radiological and nuclear research away from DNDO into S&T. The committee, under then-Chairman

[1] DHS Fiscal Year 2011 Budget in Brief, ICE 10–2647.000474. p. 139.

Thompson, worked to make this transition happen, and we believe that research and development, and operations and procurement, are best left to separate organizations in order to avoid the obvious conflict of interest.

What I hope we are going to hear today is how DNDO's mission can be better-defined. Some claim there is still confusion as to whether it is an end-to-end RDT&E and procurement entity for all things nuclear/radiological, a development entity, or an operational entity, and question whether there is an inherent conflict of interest when an agency is both an R&D workshop and a procurement platform.

Let me finish with this thought, completely out of the policy arena. On the ground, and every day, our nuclear deterrence effort requires motivated and vigilant officers supplied with the best equipment and intelligence we can give them. Customs and Border Patrol officers working at our Nation's ports of entry have an extremely complex and difficult job.

Thousands of decisions are made every day to clear a container or personal vehicle for transit into the United States, require further inspection, or even deny entry or interdict such a vehicle or person, and that is the hard, cold, every-day reality of our mission to prevent this kind of violent nuclear attack.

We must do our best.

I look forward to hearing from our witnesses today and with that, Mr. Chairman, I yield back.

Mr. LUNGREN. I thank the gentlelady for her comments, and I think the panel can tell that we are on the same page at looking at what the progress has been since our last hearing.

General L. Eric Patterson was appointed director of the Federal Protective Service, a subcomponent of the National Protective—Protection and Programs Directorate, in September 2010. He previously served as the deputy director of the Defense Counterintelligence HUMINT Center at the Defense Intelligence Agency.

Prior to joining DIA Mr. Patterson served as a principal with Booz Allen Hamilton where he supported two of the Defense Technical Information Center analysis centers, one focused on information assurance and the other on the survivability and vulnerability of defense systems. He is a retired United States Air Force brigadier general with 30 years of service.

Mr. Mark Goldstein is the director of physical infrastructure issues at GAO. Mr. Goldstein is responsible for the agency's work in Federal property and telecommunications. A former award-winning journalist and author, his other public service work has included roles as chief of staff to the D.C. Financial Control Board and senior investigative staff to the Senate Committee on Governmental Affairs.

Dr. James Peerenboom is the associate director of the decision and information sciences division at the Argonne National Laboratory, near Chicago, Illinois. In this role he is responsible for leading multidisciplinary teams of scientists and engineers in developing innovative solutions for infrastructure assurance, systems analysis, decision and risk analysis, and advanced modeling and simulation problems.

For the past 15 years he has focused on critical infrastructure protection and resilience issues, providing technical support to the Departments of Energy and Homeland Security, the President's commission on critical infrastructure protection, and White House Office of Science and Technology Policy. He received his Ph.D in energy and environmental systems from the Institute of Environmental Studies and an M.S. and B.S. in nuclear engineering from the University of Wisconsin at Madison.

Gentlemen, we ask you—well, we would first indicate that your written testimony will be made a part of the record and would ask

that you summarize your testimony with any additions as you wish in 5 minutes, and then we will have a round of questioning.

So the Chairman would recognize Director Patterson to begin.

STATEMENT OF L. ERIC PATTERSON, DIRECTOR, FEDERAL PROTECTIVE SERVICE, DEPARTMENT OF HOMELAND SECURITY

General PATTERSON. Good morning. Thank you, Chairman Lungren, Ranking Member Clarke.

My name is Eric Patterson and I am the director of the Federal Protective Service within the Department of Homeland Security's National Protection and Programs Directorate. I am honored to appear before you today to discuss FPS's progress in addressing some historically identified challenges.

FPS's mission is to protect more than 9,000 Federal buildings throughout the United States and its territories and the 1.4 million Federal employees and visitors who occupy and conduct business in them every day. We execute this mission by providing proactive law enforcement, investigations, protective intelligence, incident response, security planning, and stakeholder engagement.

Based upon my experience in the ever-changing threat environment, my belief is that risk assessment is a continuous process and not a static event. Our law enforcement and physical security professionals continually provide access risk and implement mitigation strategies through their daily activities.

During fiscal year 2011 FPS investigated and mitigated more than 1,300 threats and assaults directed towards Federal facilities and their occupants, made close to 2,000 arrests, responded to 53,000 incidents, and prevented the entry of hundreds of thousands of prohibited items into Federal facilities. FPS also conducted 1,800 Operation Shield exercises, 150 Covert Test operations, over 80,000 post inspections, and also validated the training of thousands of protective security officers that we oversee.

Over the past year FPS developed an important partnership with Argonne National Lab resulting in the completed development and current deployment of a new facility security assessment tool, called the modified infrastructure survey tool, or MIST. MIST will enable comprehensive and consistent FSAs that will allow Federal tenant agencies to make informed security and risk management decisions. The MIST tool is a welcome addition to FPS's portfolio of on-going facility assessment efforts and strategies.

As GAO has indicated, FPS employed the best project management principles in the development of MIST. MIST requirements were developed leveraging the knowledge obtained from our long-standing relationships with the General Services Administration, the Facility Security Committee, and other customers.

As we move to measure and assure the successful performance of MIST my plan is to build upon this foundation to improve FPS's management of other significant programs—for example, our protective security officer program. Just as technology is enhancing our risk assessment processes, I plan to better leverage technology to allow for more effective oversight of our contract PSOs.

A key enabler of these actions will come from the good work of our collaboration with the Systems Engineering and Design Insti-

tute, SEDI, a Federally-funded research and development center. We have engaged the SEDI to produce a full mapping of FPS activities and to then align them with FPS's current fee structure. That work will be used to produce an activity-based cost model for FPS.

These efforts are designed to result in a more efficient revenue structure for FPS and greater transparency on security costs for FPS stakeholders.

I am also pleased to note that some of our recent progress includes an increased participation in the important work of the Interagency Security Committee to include chairing a new ISC working group which will look at the future of Federal workplace security and the newly reconstituted Training Subcommittee.

FPS's program—progress in the past year and our path forward leveraging partnerships and technology is clearly in direct support of our long-term vision. It will continue to take time, deliberate planning, and the dedication of our employees and partners to fully realize our vision and I look forward to keeping you apprised of our progress.

Again, thank you for the opportunity to discuss FPS with you today, and I would be happy to answer any questions you might have.

[The prepared statement of Mr. Patterson follows:]

PREPARED STATEMENT OF L. ERIC PATTERSON

JULY 24, 2012

Thank you Chairman Lungren, Ranking Member Clarke, and the distinguished Members of the subcommittee. My name is Eric Patterson, and I am the Director of the Federal Protective Service (FPS) within the Department of Homeland Security's (DHS) National Protection and Programs Directorate (NPPD).

I am honored to appear before you today to discuss NPPD/FPS's progress in utilizing key protection and risk management practices such as allocation of resources, leveraging technology, and enhancing information sharing and coordination.

The GAO has raised several areas that have historically represented challenges for FPS including:

1. Absence of a risk management program;
2. Addressing key human capital issues through a strategic human capital plan;
3. Contract Guard workforce management and oversight; and
4. Need for a review of FPS's fee design.

Today's hearing is an opportunity to address the progress FPS has made during the past year in working to address these challenges, and to also provide information on the topics addressed in GAO's new report related to risk assessment and Protective Security Officer (PSO) program management and oversight.

FPS BACKGROUND

FPS's mission is to protect more than 9,000 Federal buildings and the 1.4 million Federal employees and visitors who occupy them throughout the country every day by leveraging the intelligence and information resources of its network of public and private-sector partners. Specifically, FPS executes its mission by providing proactive law enforcement, investigation and protective intelligence and information sharing services, incident response, security planning, and stakeholder engagement. Prior to its transfer to NPPD in 2009, FPS was organized under Immigration and Customs Enforcement and prior to that, under the General Services Administration (GSA).

Part of our core mission is to assess the threat picture for the Government Facilities Sector (GFS) and share that information with stakeholders as appropriate. For example, FPS leverages the Homeland Security Information Network (HSIN), a secure, trusted web-based portal to share information with our more than 900 Government and industry partners. One of the recent information-sharing initiatives FPS has implemented to assist in the protection of facilities and their occupants is the Federal Facility Threat Picture (FFTP), which is an unclassified assessment of the

current known threats to the facilities FPS protects. Produced quarterly, the FFTP supports the threat component of a Federal Security Assessments (FSA) and informs our stakeholders of potential threats to Government facilities. The FFTP focuses on the threats posed by a variety of actors that may seek to attack or exploit elements of the GFS. The information used in the FFTP comes from intelligence and law enforcement community reporting.

During fiscal year 2011, FPS:

- Investigated and mitigated more than 1,300 threats and assaults directed towards Federal facilities and their occupants;
- Disseminated 331 threat- and intelligence-based products to our stakeholders, 142 of which were FPS-produced;
- Conducted 81,125 post inspections;
- Interdicted more than 680,000 weapons/prohibited items including knives, brass knuckles, pepper spray, and other items that could be used as weapons or are contraband such as illegal drugs, at Federal facility entrances during routine checks;
- Made 1,975 arrests;
- Responded to 53,000 incidents involving people or property; and
- Conducted more than 1,800 high-visibility operations under Operation Shield and 150 risk-based Covert Test operations, ensuring the protection of Federal buildings and infrastructure.

FPS IS DEVELOPING A RISK MANAGEMENT PROGRAM

In terms of a risk management program, FPS's operational activities are organized by the National Infrastructure Protection Plan's (NIPP) Risk Management Framework, which calls for the following steps: Set Security Goals, Identify Assets and Functions, Assess Risks, Prioritize, Implement Protective Programs, and Measure Effectiveness. One area of recent significant progress related to risk assessment and the implementation of a risk management program is the on-going implementation of FPS's solution for conducting FSAs using an automated assessment tool. In May 2011, the decision was made to cease development of the legacy application known as the Risk Assessment and Management Program (RAMP) and to pursue a stand-alone assessment tool, in order to provide completed FSAs to customers. That decision has since been affirmed by the Department's Office of Inspector General (OIG).

In the interim period, our employees have continued their daily interactions with tenant agencies and oversight of facility security. Our personnel have been completing Pre-Modified Infrastructure Survey Tool (MIST) worksheets to enable complete FSA reports, and are constantly assessing risks to Federal facilities. Specifically, the pre-MIST worksheet allows the inspector to collect key information that will be populated into MIST and used in generating a final FSA report. Such data includes facility information, vulnerability assessments, and existing protective measures.

After consideration of several alternatives, FPS partnered with NPPD's Office of Infrastructure Protection (IP) to leverage a proven assessment methodology called the Infrastructure Survey Tool (IST). In October 2011, NPPD issued a task order to Argonne National Laboratory (ANL) through the Department of Energy to modify the existing Link Encrypted Network System (LENS) and IST for FPS use to conduct FSAs. Because this project leveraged existing tools and had limited resources and time constraints, the acquisition life cycle was tailored to meet delivery deadlines.

I am pleased to note that in its draft report, GAO noted FPS's use of project management principles in the development of MIST. Throughout the project, the MIST Users Working Group has remained engaged to ensure user involvement in the process. User feedback from field testing was uniformly positive about MIST and the FPS Gateway, confirming suitability to support the FPS mission. The MIST and FPS Gateway development efforts were completed on schedule, with ANL delivering the system to the Government on March 30, 2012. In April 2012, and the decision was made to proceed and deploy MIST. It is important to note that throughout the development and testing of MIST, field employees and our union were involved and actively participated as subject matter experts in the process.

FPS developed and is currently implementing a distance learning-based training program for each MIST user, as GAO commended in its draft report. Supervisors completed this training in April 2012 and Inspectors began their virtual training in May 2012, with completion of all training anticipated for late September 2012. This provides a hands-on learning environment for our Inspectors; they will receive virtual instruction as they use the tool in the learning environment. Once an Inspector

completes the training and successfully briefs his or her supervisor on a completed FSA, that Inspector will be able to proceed with conducting FSAs and reporting the results to a Facility Security Committee.

In leveraging existing technology in developing MIST, FPS was able to incorporate the ability to illustrate the impact of alternative countermeasures on a particular vulnerability. MIST will also show how a facility is or is not meeting the baseline level of protection for its Facility Security Level as set forth in the ISC's Physical Security Criteria for Federal Facilities standard and the ISC's Design Basis Threat report. This will lead to a more informed and better dialogue with tenants and Facility Security committees as FSA results are discussed and alternatives are explored. Additionally, FPS recently disseminated guidance Nation-wide on the commencement of the use of MIST to generate FSAs upon completion of inspector training. The anticipated results of the use of MIST are consistent assessment results Nation-wide and informed decision-making regarding security investments on the part of tenant agencies.

FPS IS ADDRESSING KEY HUMAN CAPITAL ISSUES THROUGH DEVELOPMENT OF A STRATEGIC HUMAN CAPITAL PLAN

In order to ensure that human resource requirements are aligned appropriately with FPS's overall mission, a Strategic Human Capital Plan is being developed in conjunction with NPPD's Human Capital Office. We are working to finalize the document; we intend to provide the plan and brief the committee when it is finalized.

FPS IS WORKING TO IMPROVE ITS PROTECTIVE SECURITY OFFICER MANAGEMENT AND OVERSIGHT

FPS is working to improve management and oversight of our over 13,000 Protective Security Officer (PSO) force. We have reviewed our operations Nation-wide and have taken steps at the National program level to ensure that performances under contracts are advantageous to the Government. We are actively working to implement the recommendations resulting from GAO and OIG reviews across the organization. Additionally, an Integrated Project Team (IPT) conducted a comprehensive review of how FPS resources the PSO oversight function and our current oversight policy.

FPS is also working with DHS's Science and Technology Directorate to develop a system for contract guard oversight and explore means of leveraging technology to ensure effective oversight of PSOs, such as automated tracking of guard post staff levels and PSO possession of the necessary credentials to stand post. Additionally, our training team is working closely with industry and Federal partners in developing a more effective training strategy for our PSOs.

FPS IS EXAMINING ITS FEE STRUCTURE IN ORDER TO REVIEW CURRENT FEE DESIGN

FPS operates through fee-based funding revenue, which is calculated based on the Federal facility tenant's square footage of occupancy and on the collection of services associated with the provisioning of reimbursable protective countermeasures. This fee-based financial structure is unique among Federal law-enforcement agencies and requires a greater degree of understanding internal operations to ensure it is properly aligned with FPS's costs.

To address this challenge, FPS is implementing a two-pronged strategy to better understand its activities and costs and recommend options for a new revenue structure. In January 2012, FPS collaborated with the Department's Systems Engineering and Design Institute (SEDI), a Federally Funded Research and Development Center managed by the DHS Science and Technology Directorate, to produce a full mapping of FPS activities and then align them with costs. That work will be used to produce Activity-Based Cost (ABC) models for FPS. Both of these efforts are designed to result in a more efficient revenue structure for FPS and greater transparency in security costs for FPS stakeholders.

CONCLUSION

Thank you again for the opportunity to provide you with an update on the progress FPS is making on a number of fronts. FPS aspires to be an exemplary law enforcement and strategic critical infrastructure protection organization. This is a vision uniformly shared by FPS leadership and operational staff, both at headquarters and in the field. I would be happy to answer any questions you might have.

Mr. LUNGREN. Thank you very much, Director Patterson. You stayed within the time wonderfully. A new record here.

Now, Mr. Goldstein, please.

STATEMENT OF MARK L. GOLDSTEIN, DIRECTOR, PHYSICAL INFRASTRUCTURE ISSUES, GOVERNMENT ACCOUNTABILITY OFFICE

Mr. GOLDSTEIN. Thank you, Mr. Chairman and Ranking Member Clarke. We are pleased to be here this morning to testify on the Federal Protective Service and its efforts to improve its security of Federal property, employees, and citizens who use these facilities.

FPS provides security and law enforcement services to over 9,000 Federal facilities managed by GSA. GAO has reported that FPS faces challenges providing security services, particularly completing FSAs and managing its contract guard program.

To address these challenges FPS spent about $35 million in 4 years developing RAMP, essentially a risk assessment and guard oversight tool. However, RAMP ultimately could not be used to do either because of system problems.

My testimony today is based on preliminary work for you, Mr. Chairman, and discusses the extent to which FPS is completing risk assessments, developing a tool to complete FSAs, and managing its contract guard workforce.

Our preliminary results indicate that: No. 1, the Department of Homeland Security's DHS Federal Protective Service is not assessing risks at Federal facilities in a manner that is consistent with standards such as the National infrastructure protection plan's risk management framework as FPS originally planned. Instead of conducting risk assessments, since September 2011 FPS's inspectors have collected information such as location, purpose, agency contacts, and current countermeasures.

This information notwithstanding, FPS has a backlog of Federal facilities that have not been assessed for several years. According to FPS's own data, more than 5,000 facilities were to be assessed in fiscal years 2010 through 2012.

However, GAO was not able to determine the extent of FPS's facility security assessment backlog because the data was unreliable. Multiple agencies have expended resources to conduct risk assessments themselves even though they also already pay FPS for this service.

Second, FPS has an interim vulnerability assessment tool, referred to as MIST, which it plans to use to assess Federal facilities until it develops a longer-term solution. In developing MIST, FPS generally followed project management best practices that GAO had developed, such as conducting user acceptance testing.

However, our preliminary analysis indicates that MIST has some limitations. Most notably, MIST does not estimate the consequences of an undesirable event occurring at a facility.

Several of the risk assessment experts GAO spoke with agreed that a tool that does not estimate consequences does not allow for an agency to fully assess risk. FPS officials stated that they did not include consequence information in MIST because it was not part of the original design and thus requires more time to validate.

MIST also was not designed to compare risk across Federal facilities. Thus, FPS has a limited assurance if critical risks at Federal

facilities are being prioritized and mitigated. We have made recommendations in this area in the past.

Third, GAO's preliminary work indicates that FPS continues to face challenges in overseeing its contract guard program. FPS developed the risk assessment and management program, RAMP, to help it oversee its contract guard workforce by verifying that guards are trained and certified and for conducting guard post inspections.

However, FPS faced challenges using RAMP for guard oversight, such as verifying guard training and certification information, and has recently determined that it would no longer use RAMP. Without a comprehensive system it is more difficult for FPS to oversee its contract guard workforce.

FPS is verifying guard certification and training information by conducting monthly audits of guard training and certification information. However, FPS does not independently verify the contractors' information.

Additionally, FPS recently decided to deploy a new interim method to record post inspections that replaced RAMP. We have not reviewed this system.

This concludes my opening remarks, Mr. Chairman. I would be pleased to address any questions you or Members of the subcommittee have. Thank you.

[The prepared statement of Mr. Goldstein follows:]

PREPARED STATEMENT OF MARK L. GOLDSTEIN

JULY 24, 2012

GAO HIGHLIGHTS

Highlights of GAO–12–943T, testimony before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies of the House Committee on Homeland Security.

Why GAO Did This Study

FPS provides security and law enforcement services to over 9,000 Federal facilities managed by the General Services Administration (GSA). GAO has reported that FPS faces challenges providing security services, particularly completing FSAs and managing its contract guard program. To address these challenges, FPS spent about $35 million and 4 years developing RAMP—essentially a risk assessment and guard oversight tool. However, RAMP ultimately could not be used to do either because of system problems.

This testimony is based on preliminary work for the Chairman and discusses the extent to which FPS is: (1) Completing risk assessments, (2) developing a tool to complete FSAs, and (3) managing its contract guard workforce. GAO reviewed FPS documents, conducted site visits at 3 of FPS's 11 regions and interviewed officials from FPS, Argonne National Laboratory, GSA, Department of Veterans Affairs, the Federal Highway Administration, Immigration and Customs Enforcement, and guard companies; as well as 4 risk management experts.

What GAO Recommends

GAO is not making any recommendations in this testimony. GAO plans to finalize its analysis and report to the Chairman in August 2012, including recommendations. GAO discussed the information in this statement with FPS and incorporated technical comments as appropriate.

FEDERAL PROTECTIVE SERVICE.—PRELIMINARY RESULTS ON EFFORTS TO ASSESS FACILITY RISKS AND OVERSEE CONTRACT GUARDS

What GAO Found

GAO's preliminary results indicate that the Department of Homeland Security's (DHS) Federal Protective Service (FPS) is not assessing risks at Federal facilities

in a manner consistent with standards such as the National Infrastructure Protection Plan's (NIPP) risk management framework, as FPS originally planned. Instead of conducting risk assessments, since September 2011, FPS's inspectors have collected information, such as the location, purpose, agency contacts, and current countermeasures (e.g., perimeter security, access controls, and closed-circuit television systems). This information notwithstanding, FPS has a backlog of Federal facilities that have not been assessed for several years. According to FPS's data, more than 5,000 facilities were to be assessed in fiscal years 2010 through 2012. However, GAO was not able to determine the extent of FPS's facility security assessment (FSA) backlog because the data were unreliable. Multiple agencies have expended resources to conduct risk assessments, even though they also already pay FPS for this service.

FPS has an interim vulnerability assessment tool, referred to as the Modified Infrastructure Survey Tool (MIST), which it plans to use to assess Federal facilities until it develops a longer-term solution. In developing MIST, FPS generally followed GAO's project management best practices, such as conducting user acceptance testing. However, our preliminary analysis indicates that MIST has some limitations. Most notably, MIST does not estimate the consequences of an undesirable event occurring at a facility. Three of the four risk assessment experts GAO spoke with generally agreed that a tool that does not estimate consequences does not allow an agency to fully assess risks. FPS officials stated that they did not include consequence information in MIST because it was not part of the original design and thus requires more time to validate. MIST also was not designed to compare risks across Federal facilities. Thus, FPS has limited assurance that critical risks at Federal facilities are being prioritized and mitigated.

GAO's preliminary work indicates that FPS continues to face challenges in overseeing its approximately 12,500 contract guards. FPS developed the Risk Assessment and Management Program (RAMP) to help it oversee its contract guard workforce by verifying that guards are trained and certified and for conducting guard post inspections. However, FPS faced challenges using RAMP for guard oversight, such as verifying guard training and certification information, and has recently determined that it would no longer use RAMP. Without a comprehensive system, it is more difficult for FPS to oversee its contract guard workforce. FPS is verifying guard certification and training information by conducting monthly audits of guard information maintained by guard contractors. However, FPS does not independently verify the contractor's information. Additionally, according to FPS officials, FPS recently decided to deploy a new interim method to record post inspections that replaces RAMP.

Chairman Lungren, Ranking Member Clarke, and Members of the subcommittee: We are pleased to be here today to discuss the Department of Homeland Security's (DHS) Federal Protective Service's (FPS) efforts to complete risk assessments of the over 9,000 Federal facilities under the custody and control of the General Services Administration (GSA) and oversee its contract guards in the absence of its Risk Assessment and Management Program (RAMP), a web-enabled facility security assessment (FSA) and guard management system. As we reported in July 2011, FPS had spent about $35 million and taken almost 4 years to develop RAMP—$14 million and 2 years more than planned—but still could not use RAMP to complete FSAs because of several factors, including that FPS did not verify the accuracy of the Federal facility data used.[1] As a result, FPS's Director decided to stop using RAMP to conduct FSAs and instead pursue an interim tool to replace it. FPS also experienced difficulty using RAMP to ensure that its guards met training and certification requirements, primarily because of challenges in verifying guards' data.[2] In June 2012, FPS also decided to stop using RAMP to help oversee its contract guard program.

For fiscal year 2012, FPS has a budget of $1.3 billion, with over 1,200 full-time employees and about 12,500 contract security guards, to achieve its mission to protect Federal facilities. As part of the FSA process, FPS generally attempts to gather and review facility information; conduct and record interviews with tenant agencies; assess threats, vulnerabilities, and consequences to facilities, employees, and the public; and recommend countermeasures to Federal tenant agencies. FPS's contract guards are responsible for controlling access to Federal facilities, screening access areas to prevent the introduction of weapons and explosives, enforcing property rules and regulations, detecting and reporting criminal acts, and responding to

[1] GAO, *Federal Protective Service: Actions Needed to Resolve Delays and Inadequate Oversight Issues with FPS's Risk Assessment and Management Program,* GAO–11–705R (Washington, DC: July 15, 2011).

[2] GAO–11–705R.

emergency situations involving facility safety and security. FPS relies on the fees it charges Federal tenant agencies in GSA-controlled facilities to fund its security services.[3]

This testimony is based on preliminary results of work we conducted for a report that we plan to issue to the Chairman in August 2012. That report will contain our final evaluation and recommendations. Consistent with the report's objectives, this statement addresses the extent to which FPS is: (1) Completing risk assessments, (2) developing a tool to complete FSAs, and (3) managing its contract guard workforce. To examine the extent to which FPS is completing risk assessments and overseeing guards without RAMP, we reviewed, among other things, FPS's current FSA procedures and data on completed and planned FSAs for fiscal years 2010 to 2012. Specifically, we reviewed FPS's FSA data aggregated from its 11 regions to determine the extent of its FSA backlog. However, we could not determine the extent of the backlog because FPS's data contained a number of missing and incorrect values which made the data unreliable. We also visited 3 of FPS's 11 regions and interviewed internal and external stakeholders including, among others, FPS, GSA, Department of Veterans Affairs, the Federal Highway Administration, Immigration and Customs Enforcement, and guard companies. We selected these 3 regions based on the number of Federal facilities in the region and their security levels, the number of contract guards in the region, and geographic dispersion. Our work is not generalizable to all FPS regions. To determine the status of FPS's efforts to develop an FSA tool, we reviewed, among other things, relevant project documents and Federal physical security standards, such as DHS's National Infrastructure Protection Plan's (NIPP) risk management framework. We also interviewed FPS officials, representatives from Argonne National Laboratory, and four risk management experts. We selected our four risk assessment experts from a list of individuals who participated in the Comptroller General's 2007 risk management forum.[4] This work is being conducted in accordance with generally accepted Government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

FPS DOES NOT CURRENTLY ASSESS RISKS AT FEDERAL FACILITIES BUT MULTIPLE AGENCIES ARE CONDUCTING THEIR OWN ASSESSMENTS

Our preliminary results indicate that, in the absence of RAMP, FPS currently is not assessing risk at the over 9,000 Federal facilities under the custody and control of GSA in a manner consistent with Federal standards such as NIPP's risk management framework, as FPS originally planned. According to this framework, to be considered credible a risk assessment must specifically address the three components of risk: Threat, vulnerability, and consequence. As a result, FPS has accumulated a backlog of Federal facilities that have not been assessed for several years. According to FPS data, more than 5,000 facilities were to be assessed in fiscal years 2010 through 2012. However, we were not able to determine the extent of the FSA backlog because we found FPS's FSA data to be unreliable. Specifically, our analysis of FPS's December 2011 assessment data showed nearly 800 (9 percent) of the approximately 9,000 Federal facilities did not have a date for when the last FSA was completed. We have reported that timely and comprehensive risk assessments play a critical role in protecting Federal facilities by helping decision makers identify and evaluate potential threats so that countermeasures can be implemented to help prevent or mitigate the facilities' vulnerabilities.[5]

Although FPS is not currently assessing risk at Federal facilities, FPS officials stated that the agency is taking steps to ensure Federal facilities are safe. According to FPS officials, its inspectors (also referred to as law enforcement security officers) monitor the security posture of Federal facilities by responding to incidents, testing countermeasures, and conducting guard post inspections. In addition, since September 2011, FPS's inspectors have collected information—such as location, purpose, agency contacts, and current countermeasures (e.g., perimeter security, access controls, and closed-circuit television systems) at over 1,400 facilities—which will be used as a starting point to complete FPS's fiscal year 2012 assessments. However, FPS officials acknowledged that this approach is not consistent with NIPP's risk management framework. Moreover, several FPS inspectors told us that they re-

[3] 40 U.S.C. § 586; 41 C.F.R. § 102–85.35; Pub. L. No. 111–83, 123 Stat. 2142, 2156–57 (2009).

[4] GAO, *Highlights of a Forum: Strengthening the Use of Risk Management Principles in Homeland Security,* GAO–08–627SP (Washington, DC: April 2008).

[5] GAO, *Homeland Security: Greater Attention to Key Practices Would Improve the Federal Protective Service's Approach to Facility Protection,* GAO–10–142 (Washington, DC: Oct. 23, 2009).

ceived minimal training or guidance on how to collect this information, and expressed concern that the facility information collected could become outdated by the time it is used to complete an FSA.

Multiple Federal Agencies Are Conducting Their Own Risk Assessments

We reported in February 2012 that multiple Federal agencies have been expending additional resources to conduct their own risk assessments, in part because they have not been satisfied with FPS's past assessments.[6] These assessments are taking place even though, according to FPS's Chief Financial Officer, FPS received $236 million in basic security fees from Federal agencies to conduct FSAs and other security services in fiscal year 2011.[7] For example, officials we spoke with at the Internal Revenue Service, Federal Emergency Management Agency, Environmental Protection Agency, and the U.S. Army Corps of Engineers stated that they conduct their own risk assessments. GSA is also expending additional resources to assess risk. We reported in October 2010 that GSA officials did not always receive timely FPS risk assessments for facilities GSA considered leasing.[8] GSA seeks to have these assessments completed before it takes possession of a property and leases it to tenant agencies. However, our preliminary work indicates that as of June 2012, FPS has not coordinated with GSA and other Federal agencies to reduce or prevent duplication of its assessments.

FPS EFFORTS TO DEVELOP A RISK ASSESSMENT TOOL ARE EVOLVING, BUT CHALLENGES REMAIN

In September 2011, FPS signed an interagency agreement with Argonne National Laboratory for about $875,000 to develop an interim tool for conducting vulnerability assessments by June 30, 2012.[9] According to FPS officials, on March 30, 2012, Argonne National Laboratory delivered this tool, called the Modified Infrastructure Survey Tool (MIST), to FPS on time and within budget. MIST is an interim vulnerability assessment tool that FPS plans to use until it can develop a permanent solution to replace RAMP. According to MIST project documents and FPS officials, among other things, MIST will:

- allow FPS's inspectors to review and document a facility's security posture, current level of protection, and recommend countermeasures;
- provide FPS's inspectors with a standardized way for gathering and recording facility data; and
- allow FPS to compare a facility's existing countermeasures against the Interagency Security Committee's (ISC) countermeasure standards based on the ISC's predefined threats to Federal facilities (e.g., blast-resistant windows for a facility designed to counter the threat of an explosive device) to create the facility's vulnerability report.[10]

According to FPS officials, MIST will provide several potential improvements over FPS's prior assessment tools, such as using a standard way of collecting facility information and allowing edits to GSA's facility data when FPS inspectors find it is inaccurate. In addition, according to FPS officials, after completing a MIST vulnerability assessment, inspectors will use additional threat information gathered outside of MIST by FPS's Threat Management Division as well as local crime statistics to identify any additional threats and generate a threat assessment report. FPS plans to provide the facility's threat and vulnerability reports along with any countermeasure recommendations to the Federal tenant agencies.

In May 2012, FPS began training inspectors on MIST and how to use the threat information obtained outside MIST and expects to complete the training by the end of September 2012. According to FPS officials, inspectors will be able to use MIST once they have completed training and a supervisor has determined, based on pro-

---

[6] GAO, *2012 Annual Report: Opportunities to Reduce Duplication, Overlap, and Fragmentation, Achieve Savings, and Enhance Revenue,* GAO–12–342SP (Washington, DC: February 2012).

[7] FPS currently charges tenant agencies in properties under GSA control a basic security fee of $0.74 per square foot per year for its security services including physical security and law enforcement activities as per 41 C.F.R. § 102–85.35.

[8] GAO–10–142.

[9] As of March 2012, FPS's total life cycle cost for MIST was estimated at $5 million.

[10] The ISC is comprised of representatives from more than 50 Federal agencies and departments, establishes standards and best practices for Federal security professionals responsible for protecting non-military Federal facilities in the United States. FPS is a member agency of the Interagency Security Committee in the Department of Homeland Security, along with other Federal agencies such as the General Services Administration, the Federal Aviation Administration, the Environmental Protection Agency, and other components within the Department of Homeland Security. The ISC has defined 31 different threats to Federal facilities including vehicle-borne improvised explosive devices, workplace violence, and theft.

fessional judgment, that the inspector is capable of using MIST. At that time, an inspector will be able to use MIST to assess level I or II facilities.[11] According to FPS officials, once these assessments are approved, FPS will subsequently determine which level III and IV facilities the inspector may assess with MIST.

FPS Increased Its Use of Project Management Best Practices in Developing MIST

Our preliminary analysis indicates that in developing MIST, FPS increased its use of GAO's project management best practices, including alternatives analysis, managing requirements, and conducting user acceptance testing.[12] For example, FPS completed, although it did not document, an alternatives analysis prior to selecting MIST as an interim tool to replace RAMP. It appears that FPS also better managed MIST's requirements. Specifically, FPS's Director required that MIST be an FSA-exclusive tool and thus helped avoid changes in requirements that could have resulted in cost or schedule increases during development. In March 2012, FPS completed user acceptance testing of MIST with some inspectors and supervisors, as we recommended in 2011.[13] According to FPS officials, user feedback on MIST was positive from the user acceptance test, and MIST produced the necessary output for FPS's FSA process. However, FPS did not obtain GSA or Federal tenant agencies' input in developing MIST's requirements. Without this input, FPS's customers may not receive the information they need to make well-informed countermeasure decisions.

MIST Has Limitations as an Assessment Tool

FPS has yet to decide what tool, if any, will replace MIST, which is intended to be an interim vulnerability assessment tool. According to FPS officials, the agency plans to use MIST for at least the next 18 months. Consequently, until FPS decides what tool, if any, will replace MIST and RAMP, it will still not be able to assess risk at Federal facilities in a manner consistent with NIPP, as we previously mentioned. Our preliminary work suggests that MIST has several limitations:

- *Assessing Consequence*.—FPS did not design MIST to estimate consequence, a critical component of a risk assessment. Assessing consequence is important because it combines vulnerability and threat information to evaluate the potential effects of an adverse event on a Federal facility. Three of the four risk assessment experts we spoke with generally agreed that a tool that does not estimate consequences does not allow an agency to fully assess the risks to a Federal facility. However, FPS officials stated that incorporating consequence information into an assessment tool is a complex task. FPS officials stated that they did not include consequence assessment in MIST's design because it would have required additional time to develop, validate, and test MIST. As a result, while FPS may be able to identify a facility's vulnerabilities to different threats using MIST, without consequence information, Federal tenant agencies may not be able to make fully-informed decisions about how to allocate resources to best protect Federal facilities. FPS officials do not know if this capability can be developed in the future, but they said that they are working with the ISC and DHS's Science and Technology Directorate to explore the possibility.
- *Comparing Risk Across Federal Facilities*.—FPS did not design MIST to present comparisons of risk assessment results across Federal facilities. Consequently, FPS cannot take a comprehensive approach to managing risk across its portfolio of 9,000 facilities to prioritize recommended countermeasures to Federal tenant agencies. Instead, FPS takes a facility-by-facility approach to risk management where all facilities with the same security level are assumed to have the same security risk, regardless of their location.[14] We reported in 2010 that FPS's approach to risk management provides limited assurance that the most critical risks at Federal facilities across the country are being prioritized and miti-

[11] FPS uses the ISC's Facility Security Level Determination for Federal Facilities to determine the facility security level (FSL). The ISC recommends that level I and II facilities be assessed every 5 years and level III and IV facilities every 3 years. According to the ISC's criteria, a level I facility may be 10,000 or fewer square feet, have fewer than 100 employees, provide administrative or direct service activities, and have little to no public contact; a level II facility may be 100,000 or fewer square feet, have 250 or fewer employees, be readily identifiable as a Federal facility, and provide district or State-wide services; a level III facility may be 250,000 or fewer square feet, have 750 or fewer employees, be an agency's headquarters, and be located in an area of moderate crime; and a level IV facility may exceed 250,000 square feet, have more than 750 employees, house National leadership, and be located in or near a popular tourist destination.

[12] GAO–11–705R.

[13] GAO–11–705R.

[14] GAO–10–142.

gated.[15] FPS recognized the importance of having such a comprehensive approach to its FSA program when it developed RAMP and FPS officials stated that they may develop this capability for the next version of MIST.

- *Measuring Performance*.—FPS has not developed metrics to measure MIST's performance, such as feedback surveys from tenant agencies. Measuring performance allows organizations to track progress toward their goals and, gives managers critical information on which to base decisions for improving their programs. This is a necessary component of effective management, and should provide agency managers with timely, action-oriented information.[16] Without such metrics, FPS's ability to improve MIST will be hampered. FPS officials stated that they are planning to develop performance measures for MIST, but did not give a time frame for when they will do so.

FPS FACES CHALLENGES IN OVERSEEING ITS CONTRACT GUARDS

Our work to date indicates that FPS does not have a comprehensive and reliable system to oversee its approximately 12,500 contract guards. In addition to conducting FSAs, FPS developed RAMP as a comprehensive system to help oversee two aspects of its contract guard program: (1) Verifying that guards are trained and certified to be on post in Federal facilities; and (2) conducting and documenting guard post inspections.[17] However, FPS experienced difficulty with RAMP because the contract guard training and certification information in RAMP was not reliable. Additionally, FPS faced challenges using RAMP to conduct and document post inspections.[18] For example, FPS inspectors we interviewed reported they had difficulty connecting to RAMP's servers in remote areas and that recorded post inspections disappeared from RAMP's database without explanation. Although we reported some of these challenges in 2011, FPS did not stop using RAMP for guard oversight until June 2012 when the RAMP operations and maintenance contract was due to expire.

In the absence of RAMP, in June 2012, FPS decided to deploy an interim method to enable inspectors to record post inspections. FPS officials said this capability is separate from MIST, will not allow FPS to generate post inspection reports, and does not include a way for FPS inspectors to check guard training and certification data during a post inspection. FPS officials acknowledged that this method is not a comprehensive system for guard oversight. Consequently, it is now more difficult for FPS to verify that guards on post are trained and certified and that inspectors are conducting guard post inspections as required.

Although FPS collects guard training and certification information from the companies that provide contract guards, it appears that FPS does not independently verify that information. FPS currently requires its guard contractors to maintain their own files containing guard training and certification information and began requiring them to submit a monthly report with this information to FPS's regions in July 2011.[19] To verify the guard companies' reports, FPS conducts monthly audits. As part of its monthly audit process, FPS's regional staff visits the contractor's office to select 10 percent of the contractor's guard files and check them against the reports guard companies send FPS each month. In addition, in October 2011, FPS undertook a month-long audit of every guard file to verify that guards had up-to-date training and certification information for its 110 contracts across its 11 regions. FPS provided preliminary October 2011 data showing that 1,152 (9 percent) of the 12,274 guard files FPS reviewed at that time were deficient, meaning that they were missing one or more of the required certification document(s). However, FPS does not have a final report on the results of the Nation-wide audit that includes an explanation of why the files were deficient and whether deficiencies were resolved.

FPS's monthly audits of contractor data provide limited assurance that qualified guards are standing post, as FPS is verifying that the contractor-provided information matches the information in the contractor's files. We reported in 2010 that FPS's reliance on contractors to self-report guard training and certification informa-

---

[15] GAO, *Homeland Security: Addressing Weaknesses with Facility Security Committees Would Enhance Protection of Federal Facilities,* GAO–10–901 (Washington, DC: August 5, 2010).

[16] GAO, *Homeland Security: The Federal Protective Service Faces Several Challenges That Hamper its Ability to Protect Federal Facilities,* GAO–08–683 (Washington, DC: June 11, 2008).

[17] A post is a guard's area of responsibility in a Federal facility.

[18] FPS's inspection requirement for level I and II facilities is two annual inspections of all posts, all shifts. The inspection requirement for level III facilities is biweekly inspections of two posts, any shift, and for level IV, weekly inspections of two posts, any shift.

[19] For example, guard training and certifications include firearms qualification, cardiopulmonary resuscitation, first aid, baton certification, and X-ray and magnetometer training.

tion without a reliable tracking system of its own may have contributed to a situation in which a contractor allegedly falsified training information for its guards.[20] In addition, officials at one FPS region told us they maintain a list of the files that have been audited previously to avoid reviewing the same files, but FPS has no way of ensuring that the same guard files are not repeatedly reviewed during the monthly audits, while others are never reviewed. In the place of RAMP, FPS plans to continue using its administrative audit process and the monthly contractor-provided information to verify that qualified contract guards are standing post in Federal facilities.

We plan to finalize our analysis and report to the Chairman in August 2012, including recommendations. We discussed the information in this statement with FPS and incorporated technical comments as appropriate. Chairman Lungren, Ranking Member Clarke, and Members of the subcommittee, this completes my prepared statement. I would be happy to respond to any questions you may have at this time.

Mr. LUNGREN. Thank you very much, Mr. Goldstein.

The Chairman now recognizes Dr. Peerenboom to testify.

STATEMENT OF JAMES P. PEERENBOOM, DIRECTOR, INFRASTRUCTURE ASSURANCE CENTER, ASSOCIATE DIRECTOR, DECISION AND INFORMATION SCIENCES DIVISION, ARGONNE NATIONAL LABORATORY

Mr. PEERENBOOM. Good morning. Thank you, Chairman Lungren, Representative Clarke, and the Members of the subcommittee for your invitation to testify here today.

In early October 2011 the Federal Protective Service engaged Argonne by funding the development of a software application called a Modified Infrastructure Survey Tool, or MIST, to be used by FPS on an interim basis to conduct facility security assessments. MIST uses a tailored set of questions that helps FPS establish a security baseline and allows for comparisons of facilities being surveyed against security standards. The MIST provides a standardized way of collecting and reporting facility information to inform decisions about security measures.

Argonne's work involved five tasks: Working with FPS to develop the MIST methodology; implementing the methodology as a release called MIST Release 1.0; developing a host site for MIST Release, called the FPS Gateway; assisting FPS, as requested, in training functions; and finally, providing help desk support to MIST operation.

By working closely with FPS inspectors, contract management staff, and leadership throughout the period of performance Argonne was able to meet all the defined requirements in the statement of work. MIST Release 1.0 and the FPS Gateway were delivered to FPS on March 30, 2012, 6 months after the program began. The products were delivered on time and within the defined budget.

Argonne greatly appreciates the opportunity to work with FPS in a collaborative manner to develop the MIST as a useful and usable interim tool for FPS personnel. Knowledgeable FPS leadership and staff were actively involved in all tasks and feedback was provided by FPS personnel in a timely manner to guide development activities. In addition, regular meetings were held with FPS director, Director Patterson, and his staff to review schedules and deliverables

[20] GAO, *Homeland Security: Federal Protective Service's Contract Guard Program Requires More Oversight and Reassessment of Use of Contract Guards,* GAO–10–341 (Washington, DC: April 13, 2010).

and to ensure that any problems encountered were identified and quickly resolved.

Finally, Argonne also wishes to thank the DHS Office of Infrastructure Protection, part of NPPD, their Protective Security Coordination Division in particular, for their collaboration with FPS, willingness to share methodologies, technology, and experience.

I appreciate this opportunity to summarize the MIST development activities at Argonne and I look forward to your questions. Thank you.

[The prepared statement of Mr. Peerenboom follows:]

PREPARED STATEMENT OF JAMES P. PEERENBOOM

JULY 24, 2012

Thank you Chairman Lungren, Representative Clarke, and the distinguished Members of the subcommittee for your invitation to testify here today.

My name is James Peerenboom, and I am the Director of the Infrastructure Assurance Center and the Associate Director of the Decision and Information Sciences Division at Argonne National Laboratory. Argonne is located just outside of Chicago and is one of the U.S. Department of Energy's largest National laboratories for scientific and engineering research. Argonne has been providing technical support to the U.S. Department of Homeland Security (DHS) since the Department was established in March 2003.

BACKGROUND

In late March 2011, the Federal Protective Service (FPS) requested a meeting with Argonne to discuss the potential for leveraging technical work that had been underway at the laboratory since 2007. The work that FPS was seeking to leverage was funded by the DHS National Protection and Programs Directorate's Office of Infrastructure Protection (NPPD/IP). Specifically, FPS was interested in exploring the option to modify an existing survey tool that Argonne had developed for NPPD/IP called the Infrastructure Survey Tool (IST). This security survey has been successfully deployed and used by DHS and its Protective Security Advisors (PSAs) to identify security measures at various critical infrastructure assets across the Nation. Argonne first met with FPS representatives in April 2011 to demonstrate IST functionality; discuss the purpose, scope, and limitations of the tool; and discuss FPS assessment needs. A series of subsequent discussions and meetings with FPS took place from April through September 2011.

DESCRIPTION OF IST

The IST is a survey tool that employs a tailored set of questions to identify for infrastructure owners and operators some of the potential security weaknesses at a given facility, establish an index value of protective measures at the facility, and provide comparisons with similar facilities. It is not a vulnerability or risk assessment tool. Rather, as a survey tool, the IST provides a consistent, transparent, and integrated assessment of a facility's current security posture. It was designed for application to many types of critical infrastructure assets—from refineries, railroad lines, and power plants to financial centers—to enable owners and operators to see how the security measures at their facilities stack up against those at facilities like theirs. While the IST is not intended to compare a facility's security to specific standards, it does provide a comparative measure to similar facilities.

The DHS customers for IST survey data are infrastructure owners and operators. The survey data, presented in an interactive dashboard, allows them to visualize how certain security-related changes, such as adding security cameras or installing fencing, alters the protective measures index value and may contribute to improved security. On the basis of feedback from the PSA community, the interactive dashboard in use by NPPD/IP has been well received by infrastructure owners and operators. In addition to providing insight and valuable feedback to owners and operators, the IST data are also used by DHS to benchmark security measures, identify protective measure gaps, and develop infrastructure protection strategies.

FPS WORK SCOPE

In early October 2011, FPS engaged Argonne by funding the development of a software application, called the Modified Infrastructure Survey Tool (MIST), to be used by FPS on an interim basis to conduct facility security assessments. As the name implies, the MIST is a modification of the existing IST developed by Argonne and deployed by NPPD/IP. The MIST uses a tailored set of questions that helps FPS establish a security baseline and allows for comparison of the facility being surveyed against security standards. MIST's methodology involves the gathering of data via an assessment question set, processing the data through an algorithm to convert the data to vulnerability measures, and the generation of outputs such as a report of those measures. Although the MIST was not designed to be an Interagency Security Committee (ISC)-compliant tool, it adheres to the ISC process and guidance as much as possible and captures elements of ISC standards. The MIST provides a standardized way of collecting and reporting facility information to inform decisions about security measures.

Argonne's work was funded through an existing Interagency Agreement (IAA) with NPPD/IP that encompassed IST-related tasks. Funds were committed under the IAA to develop, test, deliver, and support MIST Release 1.0. More than half of the funds were used for hardware and software to establish a web portal, called the FPS Gateway, that allows for sharing of information products and knowledge in real time. The FPS Gateway leverages the architecture and hardware/software technology of the Linking Encrypted Network System (LENS), a similar portal that Argonne developed for NPPD/IP.

Argonne's statement of work under the IAA with FPS included five tasks, all of which involved leveraging the experience, expertise, and technology used in developing the IST:

- Working with FPS to develop the MIST methodology;
- Implementing the methodology as MIST Release 1.0 (software development);
- Developing a host site for MIST Release 1.0 (i.e., the FPS Gateway);
- Assisting FPS, as requested, in training functions; and
- Providing "help desk" support for MIST operation.

PROJECT RESULTS

By working closely with FPS inspectors, contract management staff, and leadership throughout the period of performance, Argonne was able to meet all defined requirements in the statement of work. MIST Release 1.0 and the FPS Gateway were delivered to FPS on March 30, 2012. The products were delivered on time and within the defined budget. Argonne continues to provide help desk support to FPS. Feedback from FPS about the MIST as an interim survey tool has been very positive.

ACKNOWLEDGMENTS

Argonne appreciates the opportunity to work with FPS in a collaborative manner to develop the MIST as a useful and usable interim tool for FPS personnel. Knowledgeable FPS leadership and staff were actively engaged in all tasks, and feedback was provided by FPS personnel in a timely manner to guide development. In addition, regular meetings with the FPS Director also were held to review schedules and deliverables and to ensure that any problems encountered were identified and quickly resolved. Argonne also wishes to thank the NPPD/IP Protective Security Coordination Division staff for their collaboration with FPS, willingness to explain and share methodologies and technology, and thorough IAA oversight.

Mr. LUNGREN. Thank you very much.

I think we may have set a record for brevity of the three panelists, and we appreciate that. I am sure all my colleagues have questions. We will start of round of questioning, and I will start with the first 5 minutes.

General Patterson, in your previous jobs, precision, accuracy, attention to detail has been extremely important. We have had concerns prior to the time you got there with the lack of those things in some of the functions that you are supposed to—that your operation is supposed to carry out.

Last July when you testified you indicated your, I think, frustration at where FPS was at that time. So how would you assess

FPS's progress to address deficiencies in the ability to conduct facility security assessments and conduct oversight and training of the contract guard program?

As I am sure you heard Mr. Goldstein, you have seen the testimony that he gave. There seems to be some concern that he expresses there. How would you judge where you are versus where you think you need to be and where you want to be in those areas?

General PATTERSON. Thank you, sir.

Well, to begin, we are at the beginning. RAMP unfortunately did not produce results that the agency had hoped that it would. So after careful review, as you are aware, I made the decision that we were no longer going to follow that path and develop a new path.

I spent quite a bit of time with our sister activity component within Homeland Security, I.P., to talk about how they look at threats, how they look at vulnerability within the private and commercial sector, and how we could leverage what they do and bring that about as quickly as we can to look how we might do that in the Federal sector.

Once I was able to look across the—at what they were doing and some of the things that some of our other partners might—were doing at the time, because we also looked at systems within S&T, and I think GSA also had a system that we were evaluating. But at the time I believe that I.P. offered us the best product, if you will, for us to move forward. That was when I was introduced to Argonne Labs and the work that they were doing for I.P. to support I.P.

I spent quite a bit of time with I.P. and Argonne Labs to assess whether or not that would be the right direction for us. In fact, that was the right—I believe that it is the right direction for us.

Now, to get to the point of our folks within the GAO assessment, it is correct that our MIST tool does not look at consequence. However, what we do is we look at vulnerability and we look at threat. We do that in a couple of ways.

In the vulnerability, we collect a lot of data to assess and to determine how vulnerable these—our facilities are to the threats that are being posed by—in a number of areas, whether it be natural disaster, whether it be criminal threat, or whether it be from the threat of terrorism.

I have also developed a very robust activity within FPS that looks at the threat picture every day. We have folks who are working with the ODNI, the Office of Director of National Intelligence, who are working with I&A at DHS, who are working with the FBI. I have several folks across the country who are working at the JTTFs as well as the fusion centers across the country to help us better understand the threat picture as we move forward pulling vulnerability and threat together.

Relative to the consequence piece, each one of the Federal agencies has a—what we call a COOP plan. It is a plan as to when there is a problem—a disaster or something the must respond to—how they will reorganize, how they will reconstitute once that event has happened. They also have something called an occupational emergency plan that we work with them—that they can leverage, and that plan is developed when an agency is either—when

they have stood up—or when they occupy a facility, or as we go in to perform our assessments.

So we have what we believe to be a fairly robust scenario, if you will, of bringing vulnerability, threat, and consequences together not necessarily in a single document, but in a process, in a plan. So when an assessment is done my MIST tool brings me the vulnerability piece; my intelligence folks—my RIAs, is what we call them, regional intelligence folks, bring forth the threat piece, and combine that with the COOP plan and the emergency occupant plan to, I think, to bring together a fairly robust product and assessment of vulnerabilities and threats to our Federal facilities.

Mr. LUNGREN. Mr. Goldstein, would you have any comments on that?

Mr. GOLDSTEIN. Thank you, Mr. Chairman.

You know, we were very pleased that FPS has made progress. Don't get me wrong, we feel that they have made some progress. The development of MIST is certainly a way forward out of the past, whether it was from the original tools of FSRS, or whether it was through the more recent tools, where they use an Excel spreadsheet and then they had the whole RAMP program. This is a way forward, and we do believe that by finally having a program the inspectors can use where they are not subjectively determining vulnerability on their own is important. We discussed it in our report.

But we do think that being able to include consequence information, as the National infrastructure program requires, is really important. In my opinion——

Mr. LUNGREN. Mr. Patterson suggests that COOP, I believe it is, or these other elements that their clients have fulfills that role. You have a disagreement with that?

Mr. GOLDSTEIN. What I would tell you is I think that you can't have a robust program without consequence information because what you are doing is essentially telling people that you have set the dinner table without telling them what the food is going to be——

Mr. LUNGREN. No, I understand. I mean, I have always looked at risk, you know, that simple equation of threat, vulnerability, and consequence. What I was trying to get at is Mr. Patterson has suggested, or stated, that he believes that you reach that with this other component of information that he receives from what I refer to as the clients—you might use another term. Is that something you would still quarrel with at this point?

Mr. GOLDSTEIN. I don't think it provides agencies and their clients the kind of information they need to make robust decisions about which countermeasures they are going to adopt and which they aren't, which have more priority than others.

Mr. LUNGREN. Okay.

Ms. Clarke.

Ms. CLARKE. Thank you, Mr. Chairman.

Director Patterson, FPS chose to modify the current Office of Infrastructure Protection's infrastructure survey tool for its new interim risk assessment tool. What other tools did FPS consider and why weren't they selected?

General PATTERSON. Yes, ma'am. I don't have the specific names of the other tools but there were a couple other tools. I know one specifically that was being developed by the Office of Science and Technology. The challenge with that particular tool was that it was still in the development phase and it was being beta tested.

One of the challenges that I believe that we were going to have was that we were not involved in setting the requirements for the tool. So therefore, we would had to have started from the very beginning to figure out, you know, whether or not our requirements were going to be met, and then if they weren't, how we were going to incorporate that.

I felt that I needed to deliver something. We had spent time, a bit of time, on RAMP. I felt that we needed to do, to move forth quickly to try to do something to ensure that we were providing our customers, our clients, an assessment product—okay, not just an assessment, but an assessment product—and I thought MIST would be the best way to do that.

Ms. CLARKE. How does FPS plan to address the limitations that GAO identified for MIST?

General PATTERSON. Yes, ma'am. For me, this is about being a marathon and not a sprint. We are going to work aggressively with the ISC, the Interagency Security Committee, to look at how we productively and efficiently and effectively incorporate all those things that the GAO has recommended and we agree that should be considered to be in the tool.

Part of the challenge that we have is that we need to look at this very, if you will, judiciously. When we evaluate or assess a facility sometimes there are 10 tenants in that facility, okay, so we have to be—we have to ensure that when we produce a report that the consequence piece of that, if you will, is going to have relevance to all of the folks in that particular facility.

So I am not exactly sure that trying to put a consequence piece into every assessment is the right avenue. So we are going to work with the ISC to see how we might develop that and work forward and move in that direction.

Ms. CLARKE. How was the decision made to award Argonne National Laboratory the contract to develop MIST? Were there other entities considered as well?

General PATTERSON. Yes. We were required to—the acquisition process required us to consider other avenues for that, and they were—the decision was to go with Argonne.

Ms. CLARKE. Okay.

Mr. Goldstein, when do you estimate that FPS will have a more robust guard oversight tool in place that can track guard certification information and offer FPS management with greater insight as to whether all of the post inspections that need to be conducted are, in fact, occurring?

Mr. GOLDSTEIN. I would judicially say that that is a work in progress. I think the Federal Protective Service has recognized that there are some vulnerabilities in their process.

They recently stopped, as of June 2012, any use of RAMP for that process; it was the last part of RAMP that was being used and they notified offices not to be using that anymore. Much of the in-

formation in that system had never been revalidated from the old cert system so there were many problems with it.

I think it is going to take some time. We have some on-going work for this committee, taking a look at guard programs, and this will be something that we evaluate how others do it and try to bring some of that information back to you and to FPS to help them as they go forward. It is not a short-term project.

Ms. CLARKE. So would you say—yes, I mean, I recognize that. But would you say they are just at the advent of——

Mr. GOLDSTEIN. I think they are at the beginning of trying to determine what they need and how to independently verify certification as well as post inspection, yes, ma'am.

Ms. CLARKE. Okay. How does FPS now track the implementation of security countermeasures that are recommended for inclusion in the facility security assessments?

General PATTERSON. I am sorry, ma'am. Can you repeat that, please?

Ms. CLARKE. Yes, sure. How does FPS now track the implementation of security countermeasures that are recommended for inclusion in the facility security assessments?

General PATTERSON. Yes, ma'am. Currently we don't have a tracking tool. It is all done manually, if you will, paper. As our inspectors go out and interface with the committees, the security committees, the facility security committees to discuss—or the agencies to discuss what countermeasures might be necessary or what—that we might recommend, at that point we work with the FSCs to implement those requirements and it is documented, but it is documented on paper at this point because don't have a digital system, if you will, to account for that.

Ms. CLARKE. Thank you, Mr. Chairman. I yield back.

Mr. LUNGREN. Gentlelady yields back.

Mr. Walberg is recognized for 5 minutes.

Mr. WALBERG. Thank you, Mr. Chairman.

Thanks to the panel for being here.

Mr. Goldstein, you have noted that MIST, as an interim tool, falls short of providing FPS the ability to do many of the things that RAMP was intended to provide. You also noted that MIST is neither compliant with DHS's own National infrastructure protection plan and the framework that it has nor standards developed by the Interagency Security Committee.

So the question I would initially ask is, why are these standards so important?

Mr. GOLDSTEIN. I think the standards are important principally because they will create a baseline, but they will also allow that baseline to be examined across the host of the Government's portfolio. FPS does not have the ability today to look at the portfolio of Government properties that it protects—some 9,000 GSA buildings—and to determine at various levels which of those facilities require the most resources.

They protect everyone, everything essentially at each level in the same way, regardless of where it is and what its function is. So therefore we have a very static approach, building by building, to protecting our Federal infrastructure when resources are obviously

very tight, and you can't leverage the resources and priorities effectively that way.

Mr. WALBERG. I mean, that being the suggestion then, I guess, Mr. Patterson, does FPS believe ISC or NIPP standards are important criteria to meet?

General PATTERSON. Oh, absolutely, sir. They are important. We are baselining those criteria.

The challenge that we have is right now, is developing, if you will, a tool that will bring all that into play——

Mr. WALBERG. But the present tool isn't compliant with any of those standards, is it?

General PATTERSON. It is not ISC-compliant because it does not take into consideration the consequence piece of the assessment, okay? However, the tool isn't compliant but our process is compliant, okay, and the process——

Mr. WALBERG. Explain that a little further.

General PATTERSON. Yes, sir. I will. The tool is no more than a product that we provide to our customer. It is a snapshot in time of what we believe to be the vulnerability, the threat, and in this case, the consequence at a particular facility, okay? We discuss each one of those elements at the out-brief when we have completed an assessment.

All right, now, that MIST tool—that MIST product—will not cover all three, but that doesn't mean that we haven't covered that with our customers, all right? So what we are trying to do is we are trying to work with the ISC to develop a product, a tool, a product that we can deliver at the end of the day, at the end of the assessment that allows them to capture all of that into one document. We can't do that today.

Mr. WALBERG. What is the time period you are expecting this tool to be developed and then fully implemented?

General PATTERSON. In my discussions with the ISC, to their knowledge there is no one out there today that has a tool that will do that, that has been proven to do that. I understand that there might be a few folks out there who think they may have a tool to do that, but no one at this point has demonstrated that they have an effective tool that brings into play vulnerability, threat, and consequence into one document, or into a process that will bring all that together and you can provide that to our clients.

So we are working aggressively with GSA, with the ISC, and others to look at how we might do that and how the community—how we can work together with the community to make that happen.

Mr. WALBERG. Mr. Goldstein, would you concur with that, that there is not a tool capable at this time, or——

Mr. GOLDSTEIN. We haven't looked at that specifically, sir. We are doing some work for this committee—just beginning that work—taking a look at assessment tools across the Federal Government and out in the broader community, and we will hopefully be able to report back on that on the near future.

Mr. WALBERG. Okay.

Mr. Patterson, I understand that MIST was developed as an interim tool to replace RAMP. What is FPS's long-term plan to replace RAMP and what is the time line for that implementation?

General PATTERSON. Yes, sir. The long-term plan is to create a tool that is ISC-compliant. I currently don't have a—I don't have a time line for that.

Again, we are going to—we are actively working with the ISC and collaborating with the ISC. We are actively collaborating with GSA to begin to look at how we will do that: What is the next step? Because we want to build upon what we have at MIST, what we have created with MIST, so that we are not recreating every time we decide to develop a new tool or a new process. We don't want to recreate that every time.

So the bottom line is is that we are going to work with the ISC and the community to look at how we move forward. I wish I could give you a better answer but I don't have a better answer at this point until we can collaboratively come together and begin to figure out the path forward.

Mr. WALBERG. Well, I see my time has expired.

Mr. LUNGREN. Mr. Richmond——

Mr. WALBERG. Thank you, Mr. Chairman.

Mr. LUNGREN [continuing]. Is recognized for 5 minutes.

Mr. RICHMOND. Mr. Patterson, I guess I need you to make a connection for me and monitor the conversation with my colleague, and you said that MIST, or whatever you are using now, the program does not have consequence in it but your process has consequence in it. Did I hear that right?

General PATTERSON. Yes.

Mr. RICHMOND. I guess I am falling short that if the process has consequence in it why can't we develop a tool that puts vulnerability, threat, and consequence into one thing? I guess I am lost on that. Can you——

General PATTERSON. Sure.

Mr. RICHMOND. Can you help me on that?

General PATTERSON. I am not debating that we can. I am just saying that I haven't found a way to do that today.

My work to this point—our research to this point—has taken us through vulnerability and threat, but incorporating the consequence piece, as we would have it within the Federal sector, is very different than you incorporate consequence necessarily into the private sector. So what we are trying to do is when we do that we want to make sure that we develop a tool that is usable, that has got credibility, and we just haven't reached that point yet.

So when I talk about the consequence piece in the process, the process is is that when we sit down and talk with our customers and with our clients we talk about their ability to reconstitute, their ability to perform if there is an event, okay, and there are certain things that they have already done.

For instance, IRS has a COOP plan. If there is an IRS—if there is an event—for instance, the airplane that flew into the IRS facility in Austin, Texas a few years ago, well the IRS had a way to reconstitute. They knew exactly what they needed to do in order to move those functions from that facility to another facility, okay?

So for them it wasn't about us bringing something to them, all right? They knew exactly what they wanted to do. They had a plan. They have a plan.

Most Federal agencies have a plan if there is a problem, if there is an event that happens that takes them away from their facility.

Mr. RICHMOND. You said most of them do. Do——

General PATTERSON. That is an assumption. I would hope all do.

Mr. RICHMOND. Okay. I guess that was going to be my next question: Do we have a good take on who has and who does not have——

General PATTERSON. No. We work with every agency—every facility, every agency that we do an assessment, we work with them on what they call the occupant emergency plan, and that is a plan to do just what we are talking about. If there is a problem—if it is a natural disaster, if it is a criminal event or a terrorism event, what will you do? We go through a myriad of scenarios with them as to what they would do. Through every assessment we work with every tenant in the facility on that plan.

Mr. RICHMOND. I remember from the last hearing we talked about that there was the inability, or we were not in a position to verify the—that the guards that were on post were trained and certified. Have we developed something to better assess whether they are trained, certified, and present on our—in our Federal buildings?

General PATTERSON. Yes. What we are doing now—we don't—clearly we need a better process. Right now it is a pen-and-paper process for us.

We were hoping—the agency was hoping that RAMP was going to resolve this or help us get a little closer to a better solution. When that didn't evolve, when that didn't work, what I had directed all of my regions to do is revert back to a paper process, if you will, working with—as our PSOs are brought on for their time to do work, or when a client—not a client, but when our contractors, if you will, when they hire a PSO to work there is a package of certifications that each of our PSOs must have. That package—those certifications are maintained by the contractor.

However, that information that is contained in those certification packages are then forwarded—is then forwarded to every one of my regions. So we have on file in our regions, if you will, that information.

Now, the challenge is how often we can get through there and continue to recertify that their certifications are up-to-date. We have 13 certifications in those files that must be certified every year, or recertified every year. So it is a huge administrative task for us to go through that and we are looking for ways that we can digitize that, we can use technology to help us with that; we are just not there yet.

Mr. RICHMOND. I see that my time has expired so I yield back. Thank you, Mr. Chairman.

Mr. LUNGREN. Thank you.

We might have time for a quick second round if anybody is interested.

Let me just recognized myself in the first instance, and that is, Mr. Goldstein, you heard Mr. Patterson's response to the question about consequence. Here is my concern—I will have Mr. Patterson answer after I ask your thoughts—when Mr. Patterson described it he talked about some of the clients, such as IRS, having an abil-

ity to reconstitute themselves. That is what they have. That is their part of this consequence.

But I thought this tool that we were trying to develop, or tools, to do threat assessment was for the purpose of establishing, by FPS, what the levels of security would be so that you would have them more in line with what the overall risk assessment was. In that regard, a consequence piece would help Mr. Patterson and his organization decide the level of security as opposed to, as you suggested, I thought, in your testimony, that it is kind of an across-the-board, everybody is treated the same.

Am I correct in what you said and the reason why the lack of consequence would affect their ability to make those decisions?

Mr. GOLDSTEIN. Yes, sir. Mr. Patterson's discussion of COOP is an important element of, obviously, responding to any disaster or any attack but it isn't directly related, I would submit, to what we are talking about, in that the need to have consequence information as part of this program, which he agrees they will eventually develop and we are simply bringing that point out, is so that agencies working with the Federal Protective Service will have guidance on how to prioritize protecting facilities themselves over a period of time.

Mr. LUNGREN. Mr. Patterson, that is what I have found is a disconnect in what you are saying. I understand—I am happy that IRS knew how to reconstitute itself, but in terms of your assessment of your operation's ability to manage your resources in tough budget times, to decide where you need to put your emphasis, where you need to have more, where you need to have less, that that assessment tool or tools are to allow you to do that as opposed to you determining exactly what IRS ought to do at this place or one of your other clients.

General PATTERSON. Yes, sir. Again, it is—from our perspective it is a huge challenge as to how we incorporate consequence into any tool.

For instance, as I stated before, every facility is different. Some facilities, they are just stand-alone agencies; and other facilities, much like the Reagan Building, there might be literally 10 to 20 different agencies with different requirements—having different requirements, and having much more, if you will, at risk than some of the other agencies in there.

So as we look across the spectrum of facilities that we have to assess what I am trying to get away from is a one-size-fits-all kind of a tool.

Mr. LUNGREN. I don't want you to do that. That is why I am trying to figure out——

General PATTERSON. Yes, sir.

Mr. LUNGREN [continuing]. Why consequence couldn't be incorporated into the tool that you use, or you have some integration at some point in time of two tools so that you have those three things together in making your risk assessment to aid you in a determination of the level of security and the prioritizing of your resources. That is all I am trying to figure out.

General PATTERSON. Yes, sir. Again, it is our intent to incorporate consequence; we are just trying to figure out, how do we do that?

Mr. LUNGREN. Okay. Ms. Clarke.

Ms. CLARKE. Thank you, Mr. Chairman.

This question is for Director Patterson and Mr. Goldstein: How does FPS track the effectiveness and performance of the security countermeasures that it has recommended? How do you actually——

General PATTERSON. We have our inspectors who visit our sites routinely, who visit Federal facilities routinely to assess the effectiveness of our PSOs. When we do post inspections that is an assessment of our contract guard force.

We also visit our camera facilities to look at whether or not they are operating, and when they are not to look, and working with the FSC to get them repaired. So this is on an on-going and continual basis, looking at all of our countermeasures on a routine basis to ensure that they are operating efficiently and effectively.

Ms. CLARKE. Would you say it is a cyclical type of regimen that your inspectors are engaged in? Because I would imagine when you look at various facilities the landscape around those facilities may change from time to time with infrastructure changes, with——

General PATTERSON. Right. I mean, you know, we can—we—from time to time we will have different tenants who move in who have different requirements, or they, like, as you just stated, ma'am, where there are facilities that may come up next to or where we have to assess whether or not—what that impact might be on a bus station, let's say, moving in next to one of our facilities. So absolutely.

But that is a continuing process for us. We don't wait for the assessment period to do that. If, in fact, we know that the city is building—has new construction going up to one of our GSA facilities we engage immediately with GSA and the tenant to find out what—and the city—to find out what is going up and what the impact might be, and what we may need to do to answer the—to see if there is going to be an additional security standard that we may have to set out as a result of that.

Ms. CLARKE. Is there, baked into the MIST system, a way of keeping track of that information?

General PATTERSON. I am sorry. Let me—is there going to be a way——

Ms. CLARKE. Yes, of, you know—over time you are going to maybe have overlays——

General PATTERSON. Yes. Yes. Our MIST system, yes, as MIST is rolled out and as we are incorporating all that information, yes, ma'am, that all will be digitized into MIST so we can go back immediately and determine, you know, what systems are there and then how we need to correct, or adjust, or whatever we need to do to those systems, yes.

Ms. CLARKE. Dr. Peerenboom, what capabilities, if any, would a more permanent tool have over FPS's interim MIST tool?

Mr. PEERENBOOM. Well, as stated by Director Patterson and Mr. Goldstein, MIST is not a risk tool. It focuses on vulnerabilities. But it was based on work done for the Office of Infrastructure Protection at DHS, the infrastructure survey tool. That provides a platform or basis by which one could expand.

In fact, within I.P. they are looking at single assessment methodologies to pull together tools and capabilities that address risk in a holistic fashion to inform decisions about security investments. The customers of Office of Infrastructure Protection are slightly different; they are the owners and operators. The IST tool that we developed and modified for FPS is applicable to all 18 critical infrastructures, so it has a broader base.

But the subset of questions and things that apply to Federal facilities is what was done for MIST.

Ms. CLARKE. What makes these capabilities necessary?

Mr. PEERENBOOM. The Office of Infrastructure Protection has a mission to provide protection and risk analysis for critical infrastructure, and so their sets of tools are designed to encompass that broad spectrum. The IST that we developed MIST from addresses part of the equation, and there are efforts underway to expand that base within Office of Infrastructure Protection. It provides a point of leverage for FPS should they decide to use that.

Ms. CLARKE. So when the risk or the vulnerabilities seem to be evolving, how do—how effective is the MIST tool, in terms of indicating for FPS what new measures need to be taken? Is it dynamic, in other words?

Mr. PEERENBOOM. Well, that is really—I should let Director Patterson speak to that issue, but MIST provides a basis for looking at the vulnerabilities to the facility and the inspectors can add in their recommendations and their understanding of the consequences of protective measures that would—not consequences, excuse me—the countermeasures that would be applicable to that facility.

The MIST tool is partly compliant with the ISC standards but it is not an ISC-compliant tool. But we certainly took that into account, and over time, should FPS decide to do that, technically it is possible to address those standards.

Ms. CLARKE. All right. Thank you.

Mr. LUNGREN. Mr. Walberg.

Mr. WALBERG. Thank you, Mr. Chairman.

Drilling down in the same board again, Mr. Peerenboom, can MIST be developed to capture consequence? Is it capable?

Mr. PEERENBOOM. Technically the answer is yes.

Mr. WALBERG. Go a little further on why you would say technically the answer is yes.

Mr. PEERENBOOM. Well, there are capabilities, as I indicated earlier, that are being developed within the Office of Infrastructure Protection, to enhance the capabilities of the infrastructure survey tool that provides the basis that MIST was developed on, and we have the capabilities to incorporate elements of consequence, but that is a decision that obviously is not ours. But technically it is feasible.

Mr. WALBERG. It is feasible, but would you say it is not the best tool?

Mr. PEERENBOOM. It depends on requirements. No, I didn't say that.

Mr. WALBERG. Okay. Okay. Thank you.

Mr. Patterson, I would applaud you and commend you for putting an emphasis on training in your tenure at FPS, and I agree

that training is a key for your force's morale and effectiveness in the process.

Last summer you stated that you were looking at different ways FPS may be able to deliver X-ray and magnetometer and weapons training. I understand there has been significant dialogue and outreach between FPS and the private sector, which may be able to better deliver the training.

Could you enlighten us at this point in time on the on-going dialogue with industry to improve guard training?

General PATTERSON. Yes, sir. Well, first of all, one of the things that I needed to do was hire a senior deputy director for training to—who could focus in on this full-time and not be a part-time duty. So I have done that. So now I have someone who is looking across the board at all the training within FPS full-time.

Now, as we look at training for our PSO force, we are actively working with NASCO, the National Association of Security Companies, to work with them and look at how we can proliferate training across 13,000 PSOs that support FPS and all of our Federal partners. It is a huge task, because when you are talking about providing services in 50 States that all have different, if you will, training requirements, okay, we have to ensure that we are doing it in such a way that we are getting the best bang for our buck.

One of the things in the National Weapons Detection Program, in magnetometers and X-ray machines, that I knew that we needed to do was to ensure that our inspectors were adequately trained, and we have done that—we are doing it. We are just about completed all of our training for our inspectors for the magnetometers and X-ray machines——

Mr. WALBERG. The additional 8 hours of training that you were——

General PATTERSON. Yes.

Mr. WALBERG [continuing]. Proposing?

General PATTERSON. That is going to be cascaded by our inspectors, by a team of our inspectors to the—to our PSO force. Working with the—kind of in a deal where we do kind-of a trained-to-trainer kind-of a thing as well so that we can also work with our—within the contractor force, within the contractor structure to, in such, certify our contractors so that they can provide some of the training, as well.

Mr. WALBERG. You feel that FPS is capable of delivering consistent training across, as you say, the 50 States and the uniqueness of each of those?

General PATTERSON. Yes, sir. Absolutely.

Mr. WALBERG. Mr. Goldstein, would you concur with that?

Mr. GOLDSTEIN. We remain concerned, sir, because the problem that brought on the need for the additional training is now more than 3 years old when GAO was able to bring bomb-making materials into 10 Federal facilities without anyone knowing and building those bombs. It has been 3 years, and the contract guards who are there to prevent things like that from happening haven't had that additional training in all of that time.

I understand that the agency is resource-constrained, but it would seem to me that this would have been a matter of the highest priority, sir.

Mr. WALBERG. Within 3 years?
Mr. GOLDSTEIN. Yes, sir.
Mr. WALBERG. Thank you.
Mr. LUNGREN. Thank you very much.
I thank all the Members for their participation.
I want to thank the witnesses for your valuable testimony. The Members of the committee may have some additional questions for our witnesses, and so we would ask you to respond to those in writing. The hearing record will be held open for 10 days, and this subcommittee stands adjourned.
[Whereupon, at 11:09 a.m., the subcommittee was adjourned.]

APPENDIX

QUESTIONS FROM CHAIRMAN DANIEL E. LUNGREN FOR L. ERIC PATTERSON

Question 1. In testimony before the House Committee on Homeland Security in November 2009, NPPD Under Secretary Rand Beers testified that NPPD was conducting a workforce needs analysis for FPS, at the request of Secretary Napolitano, to ensure that FPS has "the right resources and staffing levels to match the missions FPS currently has." Under Secretary Beers further stated that when the results of the study were complete, Congress would be notified.

What were the results of the analysis?

Answer. The Federal Protective Service (FPS) conducted a workforce needs analysis between 2009 and 2010 and the results were used internally within the Department of Homeland Security. The results were a first step but did not fully meet the needs of the Service. FPS currently has a Federally Funded Research and Development Center on contract to conduct an activities analysis to refresh the past assumptions and requirements so that FPS may evaluate staffing levels in future years. FPS will brief the committee on the completion of the updated analysis.

Question 2a. While FPS is taking positive steps to improve the standardization and consistency of FPS, there are still concerns that FPS operates differently from region to region and lacks consistent standards.

Is consistency throughout the regions a concern of yours?

Question 2b. What steps are being taken to improve consistency of FPS from region to region?

Question 2c. Is headquarters assignment a prerequisite for promotion at FPS, and if not, do you think that would improve standardization and consistency of FPS policies?

Answer. The Federal Protective Service (FPS) is performing an activities analysis to understand and document where it should introduce or modify policies to increase operational effectiveness and reduce risk. Several variables, including geography, law, threat, and a specific customer, could warrant differences in operational activities across regions. Through FPS's current detailed review of functions and activities, it is identifying commonalities and best practices to inform uniform National policies where it makes sense to do so. FPS would be pleased to provide a detailed briefing on this effort and highlight policy and process improvements that are being implemented Nation-wide.

In addition, FPS has taken steps to realign its workforce to effectively map personnel resources to program functions. The result of this effort was the creation of an Area Management Concept, which compartmentalizes reporting for 11 regional-level offices into three Field Operations. Each Field Operation, led by a Senior Executive Service-level Assistant Director, provides oversight for multiple regional offices to help ensure standardization and consistency across the service. This area concept is a geographic-based structure that streamlines operational reporting through consolidation of information channels.

An assignment to headquarters is not a prerequisite for promotion at FPS. The creation of the Area Management Concept, led by three Senior Executive Service-level and field-based Assistant Directors, is providing standardization and consistency across the service.

QUESTIONS FROM RANKING MEMBER YVETTE D. CLARKE FOR L. ERIC PATTERSON

Question 1. According to GAO, FPS spent $795 million on its contract guards in fiscal year 2011 which represented 90% of the agency's procurement budget. How much is FPS obligated to spend on its contract guards in fiscal year 2012, and what are the projected expenditures for fiscal year 2013?

Answer. The Federal Protective Service (FPS) obligated $755.6 million on its guard contracts in fiscal year 2011, which represented approximately 91 percent of

its total contract obligations. FPS projects that it will obligate approximately $764.6 million in this program in fiscal year 2012. This projection is based on the known fiscal year 2012 obligations to date ($750.9 million as of August, 10, 2012), plus additional expected obligations through September 30, 2012, totaling $13.7 million for recurring guard services and pending modifications and/or equitable adjustments under existing contracts. FPS projects that it will obligate approximately $784.4 million in fiscal year 2013. This projection is based on the estimated escalation of the fiscal year 2012 obligation by 2.6 percent, which accounts for estimated inflationary factors such as Service Contract Act wage adjustments. However, FPS may obligate additional amounts in fiscal year 2013 as necessary to account for emerging requirements for existing and new customers and any changes that may arise concerning guard requirements.

Question 2. Why is it that as of June 2012, a total of $652,000 was spent on MIST, which appears to be useful so far, while RAMP has yielded no tangible results after four years and $35 million or more in expenditures?

Answer. The Risk Assessment and Management Program (RAMP) experienced significant programmatic and technical issues, primarily related to insufficient user involvement in the requirements definition and testing of the application, as well as the lack of an approved program baseline to control and measure program progress.

The efforts to develop and field the Modified Infrastructure Survey Tool (MIST) have been more successful because the program benefited from leveraging an existing software application already in service with the Office of Infrastructure Protection. MIST and its development addressed the shortcomings experienced within RAMP by instituting program management best practices to provide adequate controls on the development effort, and ensuring user involvement in the development and testing of MIST.

Question 3. Given that FPS had a June 2012 deadline to decide what to do with the data remaining within RAMP, what decision has been made? If a decision has yet to be made, what are the next steps?

Answer. The June 2012 deadline was tied to the expiration of the sustainment support contract for the legacy Risk Assessment and Management Program (RAMP) application. The expiration of that contract does not equate to a loss of data, as the Government owns the rights to the software and RAMP is currently installed within the Department of Homeland Security (DHS) Data Center 1 production environment.

The Federal Protective Service (FPS) has examined the data within RAMP and identified three major data sets that needed to be retained: The RAMP repository, which is a library of historical assessments and policy documents; Protective Security Officer (contract guard) contracting information; and guard post inspection reports. Data from all other modules within RAMP is either resident elsewhere within FPS or lacks value due to problems with RAMP functionality.

FPS has decommissioned RAMP as of July 12, 2012. With user access no longer available, the final data set was copied to FPS servers to ensure retention of the data. FPS will continue to work to dispose of the RAMP application during the fourth quarter of fiscal year 2012 and remove the application and all data from the DHS Data Center 1.

QUESTIONS FROM RANKING MEMBER YVETTE D. CLARKE FOR MARK L. GOLDSTEIN

Question 1. How will the security of Federal facilities be affected if FPS inspectors and law enforcement security officers are not adequately trained to use MIST?

Answer. The protection of Federal facilities may be significantly hampered if FPS's law enforcement security officers do not receive training on the Modified Infrastructure Survey Tool (MIST). As we reported in August 2012, FPS is not assessing risk at Federal facilities but plans to resume assessing Federal facilities vulnerabilities with MIST. However, if FPS's law enforcement security officers do not receive MIST training and no other alternative assessment tool is used, the backlog of facilities not assessed will increase significantly. According to FPS data, more than 5,000 facilities were to be assessed in fiscal years 2010 through 2012.

Question 2. What tools or options would be available to FPS in the event that MIST training is not completed?

Answer. FPS may be able to use other tools if it cannot use MIST to assess Federal facilities. For example, one tool is the Federal Security Risk Manager (FSRM), which FPS used from 2000 to 2009. However, FPS has experienced problems using FSRM. Another potential tool is the Integrated Rapid Visual Screening developed by DHS's Science and Technology Directorate (S&T). The IRVS is a risk assessment

tool that assesses risk using threat, vulnerability, and consequence. According to an S&T official, the IRVS is available to FPS at no cost.

Question 3. Will the implementation of MIST and other FPS activities allow for enhanced compliance with the Interagency Security Committee standards?

Answer. FPS has taken some steps to better align MIST with the Interagency Security Committee (ISC) standards. For example, MIST uses the ISC recommended countermeasures for defined threat scenarios for each facility security level.

QUESTIONS FROM RANKING MEMBER YVETTE D. CLARKE FOR JAMES P. PEERENBOOM

Question 1. What are the costs associated with developing and implementing MIST as the interim replacement for RAMP?

Answer. Argonne developed the Modified Infrastructure Survey Tool (MIST) under an existing Interagency Agreement (IAA) with the U.S. Department of Homeland Security National Protection and Programs Directorate's Office of Infrastructure Protection (NPPD/IP). Similar methodologies and technologies developed by Argonne for NPPD/IP, such as the Infrastructure Survey Tool (IST), were leveraged to reduce MIST development time, cost, and risk. A total of $850,000 was committed under the IAA to build on the foundation established for the IST to develop, test, and deliver MIST Release 1.0. More than half of the funds were used for hardware and software to establish a web portal, called the FPS Gateway, that allows for sharing of information products and knowledge in real time. The FPS Gateway leverages the architecture and hardware/software technology of the Linking Encrypted Network System (LENS), a similar platform that Argonne also developed for NPPD/IP. Work on the project was initiated on October 3, 2011. Argonne delivered MIST Release 1.0 and the FPS Gateway to FPS on March 30, 2012.

Question 2. Are there any features within RAMP that can be adapted for use with MIST?

Answer. Argonne was not tasked to evaluate RAMP and its features.

Question 3. What are the projected costs and time table for the completion of MIST?

Answer. The scope of work for MIST development was completed, and MIST Release 1.0 and the FPS Gateway were delivered to FPS, on March 30, 2012. The products were delivered on time and within the defined budget. Future enhancements to MIST, if any, and Argonne's potential role in completing such enhancements are unknown.

Question 4. Do you anticipate any cost overruns with regard to MIST?

Answer. No cost overruns were associated with Argonne's development and delivery of MIST Release 1.0 and the FPS Gateway.