Testimony of

Deputy Secretary Jane Holl Lute

U.S. Department of Homeland Security

Before the

United States Senate

Committee on Homeland Security and Governmental Affairs

March 21, 2013

Introduction

Good morning Chairman Carper, Ranking Member Coburn, and distinguished Members of the Committee. I appreciate the opportunity to appear before you today to discuss the progress the Department of Homeland Security (DHS) has made since its creation in 2003 and the challenges that confront the Department. Specifically, I will focus on the Department's success in implementing the recommendations of the Government Accountability Office's (GAO) biennial High Risk Series Update and the work we must undertake in order to more efficiently secure the safety of our Nation's citizens.

As we approach the ten-year anniversary of DHS operations, our Nation is more secure than it was ten years ago. We have progressed on every front, using the lessons of experience to become more resilient to terrorist attacks as well as to threats and hazards of all kinds.

The DHS mission is clear: create a safe, secure, and resilient place where the American way of life can thrive. In order to meet that mission, DHS must do the following:

- Prevent terrorism and enhance security;
- Secure and manage our borders;
- Enforce and administer our immigration laws;
- Safeguard and secure cyberspace; and
- Ensure resilience to disasters.

We do not do this alone. While DHS plays a central role in the effort to ensure the safety of our Nation, we rely heavily on our partners in homeland security, including our partners at the Federal level; our state, local, tribal and territorial governmental partners; non-governmental organizations like faith-based, and non-profit groups and private sector industry; and most importantly, individuals, families, and communities, who continue to be our greatest assets and the key to our success. Together we form the homeland security enterprise and through continued partnership, we leverage our shared capabilities to secure America.

DHS's Relationship with the GAO

We take our responsibilities to Congress very seriously. The GAO, an arm of Congress, is one of our essential partners. In many cases, GAO audits, investigations, and reports borne out of congressional guidance provide solid recommendations on improving management and operations at DHS. Indeed, the Department and Components tend to agree with many GAO recommendations, and work diligently to close out recommendations that provide the Department with a clear understanding of the requirements necessary for full implementation.

Both DHS and GAO have benefitted from the open line of communication we have put in place over the past four years. The culture of engagement, responsiveness, and mutual respect is the result of hard work on the part of both agencies. Today I am proud to say that our relationship with GAO has never been better.

Maintaining and improving this important relationship requires ongoing efforts to ensure that we continue to make progress. For that reason, DHS and GAO senior leaders meet at least quarterly to ensure continued progress and to address emerging issues.

Since we began meeting regularly, the number of open GAO recommendations for DHS has steadily decreased as the Department has successfully addressed and closed out more recommendations. During 2011 and 2012, GAO issued a total of 327 recommendations, and DHS closed 654 recommendations (including some from prior years). We will continue to work with GAO to close out the many recommendations we believe DHS has already implemented, including several referenced in the latest GAO High Risk Series Update. The Department is grateful for the level of coordination and professionalism displayed in our work together.

GAO's biennial High Risk Series Update provides an important opportunity to evaluate just how far we have come as a Department and how far we have yet to go. We have worked hard to demonstrate sustained improvement on the areas of greatest concern to Congress and are proud of the progress we have made since the issuance of the last High Risk Series Update. In its most recent High Risk Series Update, GAO lists the following four areas in which DHS is the lead Federal agency:

- Strengthening Department of Homeland Security Management Functions;
- Establishing Effective Mechanisms for Sharing and Managing Terrorism-Related Information to Protect the Homeland;
- Protecting the Federal Government's Information Systems and the Nation's Cyber Critical Infrastructures; and
- National Flood Insurance Program.

While we work with and support other Federal agencies on items included in the High Risk Series Update, my testimony today will focus on the progress we have made in these key areas, and the work that remains.

Strengthening Department of Homeland Security Management Functions

The creation of DHS presented a series of enormous challenges, many of which were described in the GAO High Risk area added in 2003: "Implementing and Transforming DHS." We appreciate GAO's acknowledgement of the significant improvement DHS has made, by narrowing the High Risk area this year, from "Implementing and Transforming DHS" to "Strengthening DHS Management Functions."

The refocusing by GAO of this High Risk category is a reflection of the Management Directorate's efforts to systematically address serious concerns raised by Members of Congress. In September 2010, GAO identified 31 recommended actions for DHS to address in order to be considered for removal from its High Risk List in the areas of management integration, financial management, Information Technology, human capital, and acquisitions program management. In January 2011, DHS created and issued the *Integrated Strategy for High Risk Management*, a comprehensive operational framework composed of 18 specific initiatives with detailed

corrective action plans for several critical management functions to address GAO's recommended actions. Since then, DHS has provided GAO with thorough periodic updates documenting the progress it is making in implementing these recommended actions. Over the past two years, the Department has made substantial progress in implementing the 18 initiatives, which should result in the systematic closure of each of GAO's 31 outcomes. The most recent update, given to GAO in September 2012, covered the status of the 18 specific initiatives, on areas such as workforce strategy, IT program governance, strategic sourcing, and business intelligence. DHS remains committed to sustaining this growing momentum over the coming years, and will continue to implement the *Integrated Strategy for High Risk Management* and regularly track the progress of the initiatives using quarterly internal progress reviews.

The High Risk Series Update mentions several areas of improvement, including acknowledgement of the considerable progress made in the area of management integration. Examples include strengthening the delegations of authority to clarify the roles between Headquarters and Components; improving the quality and integrity of financial statements; implementing the framework for Integrated Investment Life Cycle Management (IILCM) to ensure that the total budget ($59.8 billion in Fiscal Year 2012) is spent wisely and efficiently; and enhancing oversight responsibility for acquisition programs and investment support to DHS's Office of Program Accountability and Risk Management.

GAO's report also mentions the need to make progress in key management areas, including acquisitions, IT, financial management, human capital, and management integration. DHS agrees, issuing the *Integrated Strategy for High Risk Management* for exactly this reason, and the results are starting to demonstrate clear success. Over the next year, DHS expects to continue to build upon this progress. Specifically, DHS plans to:

- Enhance IT infrastructure by continuing to consolidate systems within DHS data centers and minimize paperwork and reporting burdens on the public;
- Continue establishing public and private cloud services to facilitate access to mission-enabling enterprise services;
- Execute the Department's Diversity and Inclusion Strategy;
- Consolidate Human Resource Information Technology efforts, including rolling out a Personnel Accountability System;
- Lead activities to increase employee engagement, morale, and leadership development;
- Continue developing a centralized business intelligence solution that will provide management information across organizational boundaries and from disparate systems to support informed decision making by Department leadership;
- Continue to improve governance through coordinated program reviews to reduce redundancies and support the Department's integrated investment management efforts;
- Develop a sustainment plan to maintain a clean audit opinion and strengthen internal controls.

I would also like to briefly mention a few accomplishments and initiatives that DHS has undertaken to address some of the areas mentioned by GAO.

Audit Opinion

In 2012, DHS earned a qualified audit opinion on all FY 2012 financial statements, a first for the Department. This full-scope audit opinion is a result of DHS's ongoing commitment to instituting sound financial management practices to safeguard taxpayer dollars. DHS also provided qualified assurance of the effectiveness of internal controls over financial reporting for the first time in its history. These efforts represent significant progress in prudent financial management.

Enhancing Acquisition Management

Over the past four years, the Under Secretary for Management led an effort to improve the Department's overall acquisition process, including reforming the early requirements development process and enhancing our ability to manage the implementation and execution of acquisition programs. As a part of these enhancements, DHS appointed Component Acquisition Executives in all Components and developed a Decision Support Tool to reduce risk and improve program performance by actively supporting programs throughout their lifecycle. The Office of the Inspector General recently acknowledged these efforts in noting that DHS has significantly strengthened its acquisition management oversight.

Small Business Contracting

DHS continues to support small businesses around the country. Since FY 2009, the Small Business Administration has evaluated agencies based on small business prime contracting, small business subcontracting, and a written progress plan. DHS has consistently received a grade of A.

Data Center Consolidation

DHS is strategically consolidating data centers to drive IT efficiencies. To date, 16 primary data centers have been consolidated, with an additional six consolidations scheduled for completion in FY 2013. At current funding, DHS expects to realize savings by FY 2020, with an anticipated overall cost avoidance of $2.8 billion by FY 2030.

Promoting Efficient Operations

Since the beginning of the Administration, DHS made an unprecedented commitment to efficiency to support our frontline operations by building a culture of fiscal discipline and accountability. Through the Efficiency Review and Component initiatives, DHS has identified more than $4 billion in cost avoidances and implemented more than 45 efficiency initiatives across the Department.

Overall, the *Integrated Strategy for High Risk Management* allows DHS to realize greater efficiencies through good management practices while also addressing the GAO High Risk designation. DHS remains committed to demonstrating measurable, sustained progress over the

coming years so that all management functions can be eligible for removal from the High Risk List.

While DHS is extremely proud of its management transformation efforts, we know that we must continue to be vigilant, and our work is not done. We appreciate GAO's partnership in our efforts. To ensure that future discussions on DHS management are as productive as possible, we should agree upon a clear definition and timeline for what constitutes sustainable and measurable progress in key management areas. Working through the *Integrated Strategy for High Risk Management*, we look forward to continuing our dialogue with GAO.

Establishing Effective Mechanisms for Sharing and Managing Terrorism-Related Information to Protect the Homeland

While we have made important progress in securing our Nation since the tragic attacks on September 11, 2001, we continue to face persistent and evolving threats. Ensuring all of those who protect the Homeland have and share the necessary information to execute our missions, while safeguarding individual privacy and civil liberties, is critical. For that reason, we have worked diligently with our homeland security partners to build a new architecture for information sharing. The four essential elements of the distributed homeland security architecture – The National Network of Fusion Centers, the Nationwide Suspicious Activity Reporting Initiative, the National Terrorism Advisory System, and the "If You See Something, Say Something" campaign – each learn from and build upon one another. These four elements require the engagement of the extended homeland security enterprise.

Fusion Centers

DHS works closely with state and local governments to support 78 state and major urban area fusion centers through personnel, training, technical assistance, exercise support, security clearances, and connectivity to Federal systems, technology, and grant funding. These state and locally owned and operated centers have become the nexus of the Federal Government's day to day information sharing efforts with state and local partners. DHS also has provided considerable resources and training to these fusion centers to support privacy and civil liberties.

Nationwide Suspicious Activity Reporting Initiative

Through the Nationwide Suspicious Activity Reporting Initiative, which is conducted in partnership with the Department of Justice, DHS works to train state and local law enforcement and homeland security partners to recognize behaviors and indicators potentially related to terrorism and terrorism-related crime; standardize how those observations are documented and analyzed; and share those reports with fusion centers and Joint Terrorism Task Forces for further analysis and investigation. Over the past four years, more than 234,000 law enforcement officers have received training under this initiative. DHS has also expanded the Nationwide Suspicious Activity Reporting Initiative to include the Nation's 16 critical infrastructure sectors.

National Terrorism Advisory System (NTAS)

In April 2011, DHS replaced the former color-coded alert system with the NTAS, which provides timely, detailed information to the public and the private sector, as well as to state, local, tribal, and territorial governments about credible terrorist threats and recommended security measures. NTAS alerts will be issued in addition to the regular intelligence and information bulletins that DHS shares with law enforcement.

"If You See Something, Say Something™"

Through the nationwide expansion of the "If You See Something, Say Something™" campaign, DHS encourages Americans to alert local law enforcement if they see something potentially suspicious. The campaign has been launched with a variety of partners, including numerous sports teams and leagues, transportation agencies, private sector partners, states, municipalities, and colleges and universities. DHS has also produced "If You See Something, Say Something™" Public Service Announcements, which have been distributed to television and radio stations across the country.

DHS's "Information Sharing and Safeguarding Strategy"

In January 2005, GAO designated terrorism-related information sharing as high risk. Since then, GAO has monitored Federal efforts to implement the Federal Information Sharing Environment (Federal ISE). The Federal ISE serves as an overarching solution to strengthening the sharing of intelligence, terrorism, law enforcement, and other information among public and private sector partners. DHS also consults with law enforcement officials from across the country to tailor the Department's products and briefings to better support state and local law enforcement and homeland security officials.

DHS's *Information Sharing and Safeguarding Strategy*, issued in January 2013, sets forth the Department's information sharing and safeguarding direction and priorities for the homeland security enterprise. It outlines goals and objectives that guide the activities of participants in the homeland security enterprise towards a common information sharing and safeguarding end within the context of our distributed homeland security architecture. Our success in gauging our performance will allow us to make decisions that are more informed during the implementation phase. This document also supports the policy positions set forth by the White House in the *National Strategy for Information Sharing* (2007), as well as the *National Strategy for Information Sharing and Safeguarding* (2012), and presents how the Department will enable its missions through sharing and safeguarding information.

DHS has made progress in both its contributions to the Federal ISE as well as executing its own information-sharing and safeguarding mission. In September 2012, GAO found that DHS has demonstrated leadership in sharing terrorism-related information to protect the homeland through its establishment and operation of the Information Sharing and Safeguarding Governance Board (ISSGB), which serves as the decision-making body for DHS information sharing and safeguarding issues. The ISSGB has enhanced collaboration among DHS Components by

identifying key information-sharing initiatives, while developing and documenting a process to prioritize initiatives for additional oversight and support.

DHS plans to address all of GAO's recommendations in our *FY 2013-2017 DHS Information Sharing and Safeguarding Strategy* ("*DHS Strategy*") and *Fiscal Years 2013-2017 Information Sharing and Safeguarding Implementation Plan* ("*Implementation Plan*"). The *DHS Strategy* and *Implementation Plan* will focus on 16 priority objectives, including a gap analysis as well as key activities and milestones to address the identified gaps. The *DHS Strategy* calls for indicators and measures that (1) assess accomplishments; (2) facilitate decision making; (3) hold DHS leaders accountable; and (4) allow the homeland security enterprise to continuously improve. Those measures will be used in the development and execution of the *Implementation Plan*. The *Implementation Plan* will allow the ISSGB to support the Department's investments in information-sharing solutions to reduce risks most effectively. DHS will update its current *Information Sharing and Safeguarding Roadmap* ("*Roadmap*") as well as the *Roadmap Implementation Guide* ("*Guide*") to track the implementation of the 16 priority objectives. The revised *Guide* and updates will also provide the Department with an institutional record to sustain ongoing implementation efforts that improve information sharing. DHS expects to develop the *Implementation Plan*, update the *Roadmap*, and revise the *Guide* by the summer of 2013.

DHS, working closely with the Federal Bureau of Investigation (FBI) and other Federal partners, has re-focused its information sharing and production efforts to better address the needs of state and local governments and private-sector partners. DHS consults with law enforcement officials from major metropolitan areas, fusion center directors, and state Homeland Security Advisors to tailor the Department's products and briefings to better support state and local law enforcement and homeland security officials.

Consistent with the direction the President has set for a robust information-sharing environment, DHS provides, in coordination with the FBI and other Federal partners, regular training programs for local law enforcement and homeland security officials to help them identify indicators of terrorist activity. In addition, DHS continues to improve and expand the information-sharing mechanisms by which front line personnel are made aware of the threat picture, vulnerabilities, and what it means for their local communities.

Protecting the Federal Government's Information Systems and the Nation's Cyber Critical Infrastructures

Cybersecurity is one of DHS's five critical missions because it is impossible to imagine a safe, secure, and resilient place where our way of life can thrive without a safe, secure, and resilient cyberspace. At the heart of securing cyberspace are two challenges, which constitute the irreducible minimum with which we must be concerned: protecting our critical infrastructure today and building a stronger cyber ecosystem for tomorrow.

DHS continues to advance its cyber analysis and warning capabilities, building its capacity to protect the Federal .gov space, and strengthening public-private partnerships and appropriate

information sharing. The United States Computer Emergency Readiness Team (US-CERT) receives and analyzes incident reports from public and private organizations, a majority of which come from outside of the Federal Government. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) provides similar analysis of incidents affecting critical infrastructure systems.

DHS's Science and Technology Directorate (S&T) is leading efforts to secure two of the Nation's major technology vulnerabilities: security weaknesses in the Internet's domain name system (DNS), and vulnerabilities in the Internet routing system. Both DNS and routing vulnerabilities can deny service to small or large portions of the Internet, make tracking and tracing Internet communications very difficult, or allow communications to be redirected without the user's knowledge. By working in a collaborative effort across Federal agencies, private industry, and global Internet owners and operators, S&T, in cooperation with the National Institute on Standards and Technology (NIST) and the Department of Commerce, leads the effort to deploy domain name security extensions, and we work with international counterparts and key technical groups to develop improvements to the standards that govern addressing and routing.

To build the stronger cyber ecosystem for tomorrow, we need to educate young individuals who can design secure systems and create sophisticated tools needed to prevent malicious acts. There is a shortage today of technically skilled people required to manage and protect network infrastructure. DHS S&T provides funding to support the National Initiative on Cyber Education (NICE) through the development and execution of cybersecurity competitions. Competitions provide a unique venue to attract talented students to a career in cybersecurity, and provide them with practical, hands-on experience in a realistic setting. In FY 2012, we saw over 1,500 students from 131 colleges and universities participate in the Collegiate Cyber Defense Competitions. Additionally, the U.S. Cyber Challenge had over 1,000 high school student participants.

Securing Federal Civilian Networks

DHS is responsible for securing unclassified Federal civilian government networks. To protect Federal civilian agency networks, DHS is deploying technology to detect and block cyber intrusions with support from the Department of Defense. In addition, DHS is responsible for coordinating the national response to significant cyber incidents and for creating and maintaining a common operational picture for cyberspace across the Government.

More than 80 percent of the time, exploits target known vulnerabilities on networks, computers, and commercial software. Until recently, most agencies did not routinely check their systems for those vulnerabilities. DHS is now deploying proven diagnostic technology across the .gov realm to automate scanning government networks every three days, enabling agencies to identify and repair the worst problems first on their networks and commercial software. This automated, Continuous Diagnostics and Mitigation (CDM) program will replace costly and infrequent manual inspections of systems.

The National Cybersecurity Protection System, also referred to as EINSTEIN, is an integrated intrusion detection, analytics, information sharing, and intrusion prevention system that uses

hardware, software, and other components to support DHS's cybersecurity responsibilities. Intrusion detection and cyber analytics capabilities are now installed at all Federal departments, allowing a more agile response to cyber threats. Additionally, the intrusion prevention service, known as E^3A, will reach initial operating capability this year, preventing known unauthorized intrusions into Federal networks. Together, these efforts will ensure that Federal cybersecurity capabilities are efficiently keeping pace with cutting-edge technologies and adapting to emerging threats.

Inter-Governmental Partnerships to Secure Networks

DHS builds partnerships with non-Federal public sector stakeholders as well to protect critical network systems. The Multi-State Information Sharing and Analysis Center (MS-ISAC) opened its Cyber Security Operations Center in November 2010, which has enhanced NCCIC situational awareness at the state and local government level and allows the Federal Government to quickly and efficiently provide critical cyber threat, vulnerability, and mitigation data to state and local governments. Since 2010, MS-ISAC has grown to include all 50 states, three U.S. territories, the District of Columbia, and more than 200 local governments.

Partnership with the Private Sector

The DHS cybersecurity approach reflects the need for ongoing collaboration at all levels of government and with the private sector. DHS works with the private sector to help secure the key systems upon which Americans rely, such as the financial sector, the power grid, water systems, and transportation networks by sharing actionable cyber threat information with our private sector partners, helping companies to identify vulnerabilities before a cyber incident occurs, and providing forensic and remediation assistance to help response and recovery after we learn of a cyber incident.

DHS's US-CERT responds to more than 100,000 incident reports each year, including multi-agency response activities for cyber incidents such as those at NASDAQ and RSA. In addition, ICS-CERT provides industry stakeholders with situational awareness and analytical support to manage risks to their computers and networks. Since it was established in 2009, ICS-CERT has deployed 20 teams to respond to significant private sector cyber incidents involving control system entities. DHS also works to empower owners and operators by providing a cyber self-evaluation tool, as well as in-person and online training sessions.

Executive Order and Presidential Policy Directive on Cybersecurity

The February 2013 Executive Order 13636 on Improving Critical Infrastructure Cybersecurity and the Presidential Policy Directive/PPD-21: Critical Infrastructure Security and Resilience also articulate a whole-of-government approach to critical infrastructure cybersecurity. These documents reinforce the need for everyone to play their parts in protecting the cyber and physical security of our critical infrastructure. Implementation efforts will drive action toward system and network security and resiliency as well as more efficient sharing of cyber threat information with the private sector. In accordance with these orders, DHS is expanding its existing information sharing efforts, including the enhanced cybersecurity services initiative and the Critical

Infrastructure Information Sharing and Collaboration Program, so that the private sector can better protect itself. Consistent with the requirements of the Executive Order, DHS is also leading the way in ensuring that privacy and civil liberties protections are incorporated into our cybersecurity initiatives. DHS is also working with NIST and the private sector to develop voluntary standards, methodologies, procedures, and processes to address cyber risks.

While DHS has made significant progress in ensuring the cybersecurity of our Nation, the Executive Order and Presidential Policy Directive are important steps towards further strengthening the Nation's cybersecurity.

DHS's Work with GAO and Congress on Cybersecurity

GAO recognized these and other accomplishments through the closure of 16 recommendations to DHS over the last year regarding cyber analysis and warning, the Trusted Internet Connections (TIC) initiative, and EINSTEIN. The tenor of GAO's High Risk report over the last six years has shifted, focusing now on a whole-of-government approach to cybersecurity as opposed to DHS-specific challenges. DHS is well positioned to support this shift in focus, and its cybersecurity strategy, *Blueprint for a Secure Cyber Future,* focuses on identifying the capabilities needed to adopt such an approach.

DHS works closely with GAO on cybersecurity. Senior NPPD and GAO officials meet quarterly to share information on ongoing cyber activities, discuss DHS's strategic direction in cybersecurity, and review the status of open recommendations. This year, DHS has provided GAO with significant documentation to close nearly all open recommendations, including those related to cyber analysis and warning, public-private partnerships, and the TIC and EINSTEIN initiatives. Where recommendations remain open, DHS has demonstrated to GAO and Congress significant progress in strengthening the effectiveness of partnerships and is continuing to support GAO's request for additional information on the NCCIC.

Congress can support our continuing progress in cybersecurity in two ways: first, you can ask GAO for a clearer articulation of its High Risk criteria so that DHS can use these criteria as a reference when working with our public and private sector partners; and second, passage of comprehensive cyber legislation would allow us to implement the full range of steps needed to build a strong public-private partnership. Secretary Napolitano and I look forward to continuing our work with you to provide the legislative framework for a truly whole-of-Nation approach to securing cyberspace.

National Flood Insurance Program

The National Flood Insurance Program (NFIP) serves as the foundation for national efforts to reduce the loss of life and property from flood disasters, and is estimated to save the Nation $1.6 billion annually in avoided flood losses. By encouraging and supporting mitigation efforts, the NFIP reduces the impact of disasters. While the NFIP has experienced significant successes since it was created more than 40 years ago, there are a number of challenges facing the program. The most significant challenge is balancing the program's affordability with its fiscal soundness. The NFIP must continue to offer affordable insurance that will properly identify those at risk and provide them adequate coverage, while reducing the need for taxpayer-financed disaster assistance.

Today, more than 21,000 communities in 56 states and territories participate in the NFIP, resulting in more than 5.6 million NFIP policies providing over $1.2 trillion in coverage. This past fiscal year, the NFIP increased the number of existing flood insurance policies by 47,992.

While the NFIP has been a successful program throughout its 42 years of existence, GAO offers helpful and instructive recommendations for improving the program and DHS/FEMA has already made great progress towards implementing these recommendations.

Flood Mapping

To directly respond to the flood-risk reduction needs of communities, FEMA has produced digital flood hazard data for more than 88 percent of the Nation's population. The NFIP floodplain management standards in each participating community can reduce flood damage in newly constructed buildings by more than 80 percent.

Prior to 2003, more than 70 percent of FEMA's flood maps were at least 10 years old. These maps were developed using what is now outdated technology, and, more importantly, many maps no longer accurately reflected current flood hazards. Over the last eight years, Congress has provided over $1 billion to update and digitize our Nation's flood maps so we better understand the risks that our Nation faces from flooding. Since the start of FY 2009, we have been implementing the Risk Mapping, Assessment, and Planning (Risk MAP) program, which not only addresses gaps in flood hazard data, but uses updated data to form a solid foundation for risk assessment and floodplain management, and to provide state, local, and tribal governments with information needed to mitigate flood-related risks. Risk MAP is introducing new products and services extending beyond the traditional digital flood maps produced in Flood Map Modernization, including visual illustration of flood risk, analysis of the probability of flooding, economic consequences of flooding, and greater public engagement tools. FEMA is increasing its work with officials to help use flood risk data and tools to communicate risk to citizens more effectively, and enable communities to enhance their mitigation plans.

FEMA also initiated 600 Risk MAP projects affecting 3,800 communities and addressed their highest priority engineering data needs, including coastal and levee areas.

Actuarial Soundness

The passage of the Biggert-Waters Flood Insurance Reform Act in July 2012 was a critical priority for FEMA. The reauthorization and reform means predictable authorization for the NFIP for the next five years. It also established Congress' intent for the NFIP to become a more fiscally sound program through risk-based rates for policy holders. The passage of this important law provides FEMA the authority to address the structural challenges that face the NFIP, and allows FEMA to phase in actuarially sound rates to previously subsidized policies and establish a reserve fund to pay claims in high-loss years.

FEMA has already begun to provide instruction to its Write Your Own insurance company partners to implement the removal of certain subsidies outlined in the law. Starting January 1, 2013, rates for subsidized non-primary residences began increasing upon renewal. In the Fall of 2013, FEMA anticipates releasing further instruction on phasing out subsidies for business properties, substantially damaged or improved properties, severe repetitive loss properties, properties that have incurred flood-related damages where claim payments exceed the fair market value of the property, and newly-purchased property.

In addition, FEMA is also working closely with our governmental partners, including GAO, the Army Corps of Engineers, and the Federal Insurance Office, on the required studies including studies on affordability, reinsurance, NFIP participation by Indian Tribes, and repayment of the NFIP debt to the Treasury.

Strategic Planning Efforts

GAO also recommends that DHS/FEMA complete a strategic plan for the NFIP. We agree with GAO on the importance of multi-year planning, as we must simultaneously execute during the current fiscal year, as well as prioritize and set targets for the upcoming fiscal year, and plan for two years out. FEMA's Federal Insurance and Mitigation Administration has developed a Leadership Guide to Multi-Year Planning that complements their published FY 2012-2014 Strategic Plan. The vision for the multi-year planning process is to ensure the NFIP aligns to FEMA's Planning, Programming, Budget, and Execution (PPBE) process designed to link budget to performance. The goals for multi-year planning include:

- Improving alignment between HQ and Regions;
- Reducing redundant efforts;
- Yielding better quality inputs;
- Preparing for PPBE data calls; and
- Taking advantage of PPBE opportunities.

Establishing a vision for its multi-year planning process and setting goals directly aligned to the Mitigation and Insurance Strategic Plan allows FEMA to better manage its performance and outputs in a time of declining resources.

Claims Management System

FEMA continues to maintain focus on its effort to modernize the NFIP insurance and claims management system. An NFIP Executive Steering Committee was established to provide executive oversight on the development of the new system. The Executive Steering Committee includes representation from a number of FEMA's senior leaders and the DHS Chief Information Officer, as recommended by GAO. Modernizing FEMA's NFIP IT system will address performance gaps by developing and utilizing modern technology to monitor the overall performance of the NFIP in real time. The modernization of the NFIP IT system will provide the necessary automation for the complex business model that the NFIP requires for use by both FEMA and its insurance partners.

While we continue to implement GAO's recommendations and make improvements to the NFIP, we believe that we have already implemented many of GAO's recommendations in this area, and look forward to continuing our close collaboration with GAO in order to close out the recommendations that we have already completed and focusing our energies on the work that remains.

Government-Wide GAO High Risk Series Areas

In addition to the GAO High Risk Series Update areas where DHS is the lead, we also work to improve our operations on several Government-wide GAO High Risk Series areas that have DHS equities, including "Strategic Human Capital Management," "Managing Federal Real Property," and the newly-created area, "Limiting the Federal Government's Fiscal Exposure by Better Managing Climate Change Risks." We will continue to make progress on the first two areas in coordination with Congress, GAO and our inter-agency partners, and look forward to a productive dialogue with Congress and GAO on this newly-created GAO High Risk area.

Conclusion

Thank you again for the opportunity to appear before you today to discuss the progress DHS has made in implementing GAO's recommendations, as well as the work we still must do in order to ensure the safety and security of our Nation.

I am happy to answer any questions you may have.