OFFICE OF INSPECTOR GENERAL

Testimony of Inspector General John Roth

Before the Committee on Oversight and Government Reform

U.S. House of Representatives

"Empowering the Inspectors General"

Homeland Security

February 1, 2017
10:00 AM

Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee, thank you for inviting me here today to discuss Inspector General challenges and recent legislative changes enacted by the *Inspector General Empowerment Act of 2016*.

The Value of Independent Oversight in Improving Government Operations

No government agency, no matter how dysfunctional, will change of its own accord. During my tenure as Inspector General for DHS, I have witnessed three agencies – FEMA, TSA, and the Secret Service – that have had to confront the necessity of changing the manner in which they do business. It is a wrenching process that no agency would undergo voluntarily. Change in a bureaucracy happens as a result of three things: a dramatic intervening event, followed by intense scrutiny of agency programs and operations, and a resultant leadership commitment to change. Independent oversight by both the Inspector General and Congress is a critical and necessary ingredient to positive, constructive change.

For example, FEMA's approach to disaster response changed only after Hurricane Katrina revealed the shortfalls in its operations, consistent IG and congressional scrutiny brought further analysis to the problem, and the administration and FEMA leadership committed to change the manner in which FEMA responded. Over time, FEMA evolved its way of doing business as evidenced by the effective and efficient response to Superstorm Sandy, as we noted in our report on the matter. It did so by proactively preparing for the storm, overcoming staffing challenges, making well-informed resource decisions, and effectively coordinating its response with other stakeholders.[1]

TSA was confronted with the need to change as a result of dramatic and troubling shortfalls discovered by our covert testing program, as well as other OIG reports about deficiencies in TSA's judgment of risk in relation to expedited screening, vetting airport employees, and managing the access badge program.[2] It was only through our oversight, oversight by this and other congressional committees, and TSA's then-new leadership strongly embracing the message, that TSA at last publicly acknowledged the need for change and

---

[1] *FEMA's Initial Response in New York to Hurricane Sandy*, OIG-13-124 (September 2013).
[2] *Vulnerabilities Exist in TSA's Checked Baggage Screening Operations*, OIG-14-142 (September 2014); *Security Enhancements Needed to the TSA PreCheck Initiative*, OIG-15-29 (January 2015); *TSA Can Improve Aviation Worker Vetting*, OIG-15-98 (June 2015); *Use of Risk Assessment within Secure Flight*, OIG-14-153 (June 2015); *Covert Testing of TSA's Passenger Screening Technologies and Processes at Airport Security Checkpoints*, OIG-15-150 (September 2015); *TWIC Background Checks Not as Reliable as They Could Be*, OIG-16-128 (September 2016); *TSA Could Improve Its Oversight of Airport Controls over Access Media Badges*, OIG-17-04 (October 2016).

started the long road to becoming a more effective organization. While there is much work to be done at TSA — and the change in TSA leadership risks stalling the momentum — as an agency it is in a far better place than it was two years ago.

As this Committee well knows, the well-publicized protective failures by the Secret Service resulted in hearings and investigations by this Committee, by my office, and by the independent Protective Mission Panel (PMP). This oversight resulted in an excruciating process of examination and self-examination, which is by no means over, about the manner in which the Secret Service does business. As a result, the Secret Service has taken steps to fix some of the systemic issues that have plagued the agency over time. As we noted in our most recent report:

> The Secret Service has clearly taken the PMP's recommendations seriously, which it has demonstrated by making a number of significant changes. However, fully implementing many of the PMP's recommendations will require long-term financial planning, further staff increases, consistent re-evaluation of the initiated actions' effectiveness, and a multi-year commitment by Secret Service and Department of Homeland Security leadership. [3]

The key to sustaining the gains made thus far is a leadership commitment by the new Administration and continued thoughtful oversight.

Oversight makes government better and fosters positive change. The critical and skeptical review of programs and operations, both by the Inspectors General and by congressional oversight committees, acts as the "disinfectant of sunlight" to ensure a more efficient government. It works in conjunction with the *Inspector General Act's* requirement that IGs keep Congress fully and currently informed of problems, abuses and deficiencies within the Department.

IG Empowerment Act Will Bring More Emphasis on Big Data

Thanks to the authorities contained within the newly enacted *Inspector General Empowerment Act (IGEA)*, we are planning more audits using "big data." DHS and the rest of the government hold vast repositories of data. Matching two disparate databases can yield valuable insights. For example, we matched a database of disaster victims who claimed not to have insurance, and thus were eligible for taxpayer relief, against a private insurance database. Using this

[3] *The Secret Service Has Taken Action to Address the Recommendations of the Protective Mission Panel*, OIG-17-10 (November 2016).

system, we identified 29,763 records where FEMA paid approximately $250 million in homeowners' assistance to Hurricane Sandy applicants whom the private insurance database identified as having made private homeowners' or automobile insurance claims. Of the 29,763 records, there were 2,289 where applicants self-certified during the FEMA application process that they had *no* property insurance, a claim that was demonstrably false. Those records may have the highest probability of being fraudulent. This exercise demonstrated the weakness in FEMA's benefit process for weeding out fraudulent claims.[4]

Previously, the *Computer Matching Act* interposed significant barriers to us matching DHS data against data contained in other government databases. For example, we compared TSA's database of SIDA badge holders, who have unrestricted access to secure areas within airports and aircraft, against the National Counterterrorism Center's Terrorist Identities Datamart Environment (TIDE) database. In matching the data, we found that there were 73 individuals with links to terrorism who were holding SIDA badges. This occurred because TSA did not have access to the complete database, which it recognized was a risk to national security, and a weakness in its system. Such data matching creates powerful insights not otherwise available, and as a result of this audit, TSA was able to successfully petition the Intelligence Community for access to the entire TIDE database.[5]

We found that actually matching the data was a relatively simple exercise, but that getting the approvals and other permissions under the *Computer Matching Act* took over 18 months to accomplish. Now, thanks to the IGEA, IG offices are no longer subject to the *Computer Matching Act* and can match data far more quickly.

Having this exemption presents an opportunity for us to plan new and creative audits and we are in the process of ramping up our capabilities in this area. The Recovery Accountability and Transparency Board (RATB), which previously provided DHS OIG with analytic support for audits and investigations, officially closed on September 30, 2015. Since June 2015, we have been proactive in leveraging our successful experience with the RATB to establish a similar analytics capacity within DHS OIG. We hired an analyst and are looking to recruit a data architect and additional data analytics personnel. We made substantial progress testing and installing the state-of-the-art suite of hardware and software needed to analyze structured and unstructured data, perform link analysis, and examine geospatial information. Further, we implemented processes and procedures to vet Disaster Relief Fund (DRF)

[4] *FEMA Faces Challenges in Verifying Applicants' Insurance Policies for the Individuals and Households Program*, OIG-16-01-D (October 2015).
[5] *TSA Can Improve Aviation Worker Vetting*, OIG-15-98 (June 2015).

contractors and assess DRF audit risks, similar to services that the RATB previously provided. In the long term, we expect to expand this in-house capability to support data analytic needs across DHS OIG on audits addressing a range of issues including border and transportation security, immigration and citizenship, budget and contract management, cybersecurity, customs enforcement, and research and development.

I thank this Committee for its leadership in championing the IGEA, and the cause of vigorous and independent oversight.

Focusing on the Right Things

DHS is a massive organization, consisting of over 230,000 employees and an equal number of contractors engaged in a broad spectrum of activities across the globe, the improper execution of which could have grave consequences to our homeland security.

By contrast, my office is very small. We represent about 0.25% of the DHS budget; in a typical budget year, DHS returns as unspent more money than our entire annual budget. We have one criminal investigator for every 2,000 employees and contractors. Our audit reach is likewise very small. In the disaster relief area, for example, we are able to audit about 70 disaster grants issued to local communities and other organizations per year. In contrast, FEMA currently manages grants for approximately 100,000 such sub-grantees.

Making the right choices about what we audit and inspect is critical. To assist in doing this, we have created a process to assess risk within the agency – something the Department itself has not yet done. In October, we established the Office of Enterprise Risk Identification and Management (OERIM) to enhance the OIG's capacity to focus its limited resources on the areas of greatest risk and impact to the U.S. public and to the Department. The office benchmarked risk-based planning with other federal agencies and developed rigorous risk identification and analysis techniques to conduct major studies across the Department.

Specifically, OERIM will:

- Build an online comprehensive knowledge library in key risk focus areas for DHS OIG auditors, inspectors, and investigators;
- Produce risk assessments in key focus areas that quantify risk and identify cross-cutting themes and trends;
- Contribute relevant data to the OIG annual planning process for prioritizing audits, inspections, and investigations based on risk; and

- Ensure the OIG itself evaluates risk in our own operations and reports our highest risks to OMB by June 2, 2017, as required by the recently revised OMB Circular A-123.

We are taking a more holistic view of DHS and are developing a rigorous process to prioritize reviews in the OIG's annual plan based on risk. If we better understand the Department's risks, particularly cross-cutting or shared risks, our office can issue high impact Department-wide recommendations to save taxpayer dollars, enhance unity of effort initiatives, and direct resources to where they will do the most good.

Priorities and Challenges

Homeland Security faces many challenges, and we at OIG have focused our energy on the major management and performance challenges. We have listed six:

- creating a unified department
- employee morale and engagement
- acquisition management
- grants management
- cybersecurity, and
- improving management fundamentals.[6]

Today, I will focus on the challenges the Department faces in acquisition management and grants management.

Acquisition Management

Acquisition management, which is critical to fulfilling all DHS missions, is inherently complex, high risk, and challenging. Since its inception in 2003, the Department has spent tens of billions of dollars annually on a broad range of assets and services — from ships, aircraft, surveillance towers, and nuclear detection equipment to IT systems for financial management and human resources. DHS' yearly spending on contractual services and supplies, along with acquisition of assets, exceeds $25 billion. There continue to be DHS major acquisition programs that cost more than expected, take longer to deploy than planned, or deliver less capability than promised. The Department was established very quickly by combining many legacy and new agencies, so DHS' earliest acquisition processes were imperfect and slow to mature. Initially, DHS operated in disparate silos focused on purchasing goods and services with minimal management of requirements. In their

[6] *Major Management and Performance Challenges Facing the Department of Homeland Security,* OIG-17-08 (November 2016).

transition to DHS, seven agencies, including the U.S. Coast Guard, FEMA, and TSA retained their own procurement functions. The expertise and capability of the seven procurement offices mirrored their pre-DHS expertise and capability, with staff sizes ranging from 21 to 346.

Although DHS has made much progress since then, it has not yet coalesced into one entity working toward a common goal. The Department still lacks uniform policies and procedures, a dedicated core of acquisition professionals, as well as component commitment to adhere to departmental acquisition guidance, adequately define requirements, develop performance measures, and dedicate sufficient resources to contract oversight.

A good example of the challenges faced can be seen in the U.S. Citizenship and Immigration Services (USCIS) efforts to automate immigration benefits. USCIS still uses a paper file system to process immigration benefits and spends $300 million per year just to store and move its 20 million immigrant paper files. USCIS has been attempting to automate this process since 2005, but has made little progress. Notwithstanding spending more than $500 million on the technology program between FYs 2008 and 2012, little progress has been made. Past automation attempts have been hampered by ineffective planning, multiple changes in direction, and inconsistent stakeholder involvement. USCIS deployed the Electronic Immigration System (ELIS) in May 2012, but to date, customers can apply online for only 2 of about 90 types of immigration benefits and services. USCIS now estimates that it will take 3 more years—more than 4 years longer than estimated—and an additional $1 billion to automate all benefit types as expected.[7]

These failures have a real impact on our national security. Because of processing errors resulting from premature release of ELIS software, USCIS received over 200,000 reports from approved applicants about missing green cards. The number of cards sent to wrong addresses has incrementally increased since 2013 due in part to complex processes for updating addresses, ELIS limitations, and factors beyond the agency's control. USCIS produced at least 19,000 cards that included incorrect information or were issued in duplicate. Most card issuance errors were due to design and functionality problems in ELIS. USCIS' efforts to address the errors have been inadequate. Although USCIS conducted a number of efforts to recover the inappropriately issued cards, these efforts also were not fully successful and lacked consistency and a sense of urgency. Errors can result in approved applicants unable to obtain benefits, maintain employment, or prove lawful immigration

[7] *USCIS Automation of Immigration Benefits Processing Remains Ineffective*, OIG-16-48 (March 2016).

status. In the wrong hands, Green Cards may enable terrorists, criminals, and illegal aliens to remain in the United States and access immigrant benefits.[8]

Finally, we issued a management alert as it related to the USCIS rollout of the N-400 form on ELIS in April of last year. The use of ELIS has impaired the ability of USCIS Immigration Services Officers and field personnel to conduct naturalization processing. In the course of our audit work, we discovered significant deficiencies in background and security checks for applicants, including 175 applicants who were granted citizenship with incomplete or inaccurate background checks.[9]

DHS has instituted major reforms to the acquisition process and has exerted significant leadership to gain control of an unruly and wasteful process. However, we worry that these reforms, if not continuously supported and enforced, could be undone. As DHS continues to build its acquisition management capabilities, it will need stronger departmental oversight and authority, increased commitment by the Department and components, as well as skilled personnel to effect real and lasting change.

Congress has previously introduced legislation designed to address DHS' acquisition challenges. We would support legislation that codifies existing policy and relevant offices; provides the necessary authority for key personnel and mechanisms within the Department to effectively manage major acquisition programs; reinforces the importance of key acquisition management practices, such as establishing cost, schedule, and capability parameters; and includes requirements to better identify and address poorly performing acquisition programs.

Grants Management

FEMA manages the Federal response to, and recovery from, major domestic disasters and emergencies of all types. In doing so, FEMA coordinates programs to improve the effectiveness of the whole community and leverages its resources to prevent, protect against, mitigate, respond to, and recover from major disasters, terrorist attacks, and other emergencies. In this role, FEMA awards an average of about $10 billion each year in disaster assistance grants and preparedness grants.

Based on the work and findings of OIG Emergency Management Oversight teams deployed to disaster sites in nearly a dozen states, we determined that

[8] *Better Safeguards are Needed in USCIS Green Card Issuance*, OIG-17-11 (November 2016)
[9] *Management Alert – U.S. Citizenship and Immigration Services' Use of the Electronic Immigration System for Naturalization Benefits Processing*, OIG-17-26-MA (January 2017)

FEMA generally responds effectively to disasters. For the disaster sites we visited, FEMA responded proactively and overcame a variety of challenges while coordinating activities with other Federal agencies and state and local governments.

However, our body of work over the past few years suggests that FEMA has not managed recovery from disasters well. Although FEMA provides grant management funding to grantees, FEMA has not held them accountable for managing subgrantees, and states and other grantees have not done well in guiding and managing subgrantees. This means the entire layer of oversight intended to monitor the billions of dollars awarded by FEMA in disaster assistance grants is ineffective, inefficient, and vulnerable to fraud, waste, and abuse. Of the $1.55 billion in disaster grant funds we audited last year, we found $457 million in questioned costs, such as duplicate payments, unsupported costs, improper procurement practices, and unauthorized expenditures. This equates to a 29 percent questioned-cost rate, which far exceeds industry norms, and it illustrates FEMA's continued failure to adequately manage grants.[10]

We also saw examples of inadequate grant management in preparedness grants. In an overarching audit of OIG recommendations related to preparedness grants, we reported that FEMA had not adequately analyzed recurring recommendations to implement changes to improve its oversight of these grants. This occurred because FEMA did not clearly communicate internal roles and responsibilities and did not have policies and procedures to conduct substantive trend analyses of audit recommendations.[11]

Although FEMA has been responsive to our recommendations for administrative actions and for putting unspent funds to better use, FEMA has not sufficiently held grant recipients financially accountable for improperly spending disaster relief funds. As of September 27, 2016, FEMA had taken sufficient action to close 130 of our 154 FY 2015 disaster grant audit report recommendations. However, the 24 recommendations that remained open contained 90 percent ($413 million) of the $457 million we recommended FEMA disallow that grant recipients spent improperly or could not support. Further, in FYs 2009 through 2014, FEMA allowed grant recipients to keep 91 percent of the contract costs we recommended for disallowance for noncompliance with Federal procurement regulations, such as those that

[10] *Summary and Key Findings of Fiscal Year 2015 FEMA Disaster Grant and Program Audits*, OIG-17-13-D (November 2016).
[11] *Analysis of Recurring Audit Recommendations Could Improve FEMA's Oversight of HSGP*, OIG-16-49 (March 2016).

require opportunities for disadvantaged firms (e.g., small, minority, and women-owned) to bid on federally funded work.[12]

Based on our recurring audit findings, it is critically important that FEMA officials examine regulations, policies, and procedures and assess the need for more robust changes throughout all grant programs. FEMA should refocus its efforts to identify systemic issues and develop solutions to address the cause and not just the symptoms. FEMA needs to improve its oversight of state grantees and proactively engage with states to improve management and guidance of subgrantees.

Protecting Whistleblowers Against Retaliation

Of course, none of the work we do is possible without the men and women in the DHS workforce, and DHS contractors, coming forward to let us know about significant claims of waste, fraud, abuse, and misconduct. We have raised our profile within DHS as the entity to which these allegations are reported, and with effective results. It is our duty to protect these individuals from being retaliated against as a result of stepping forward. In an average year, we receive about 175 claims of whistleblower retaliation.

DHS OIG investigates allegations of whistleblower reprisal made by uniformed United States Coast Guard members; DHS contractors, subcontractors and grantees; and DHS employees. Our Whistleblower Protection Unit (WPU) conducts investigations under the authority of the *Inspector General Act of 1978*, as amended, and pursuant to the *Military Whistleblower Protection Act*, 10 U.S.C. § 1034, Presidential Policy Directive 19, and the *Pilot Program for Enhancement of Contractor Protection*, 41 U.S.C. § 4712. Investigations under these statutes are mandatory by DHS OIG when a prima facie case of reprisal is alleged. Additionally, in certain cases, DHS OIG conducts investigations pursuant to the *Whistleblower Protection Act*, 5 U.S.C. § 2302.

In the last year, DHS OIG undertook a substantial reorganization and rebuilding of its whistleblower protection function by creating a new and dedicated WPU housed in our Office of Counsel. The WPU consists of the Whistleblower Ombudsman, a supervisory whistleblower investigator and two newly hired whistleblower administrative investigators. The WPU has primarily been responsible for intake and preliminary complaint review during this timeframe, while Special Agents from the DHS OIG Office of Investigations and attorneys from the Office of Counsel jointly conduct all whistleblower investigations that are opened.

[12] *FEMA Can Do More to Improve Public Assistance Grantees' and Subgrantees' Compliance with Federal Procurement Rules*, OIG-16-126-D (September 2016).

We are confident that these changes will make us more effective; however, we acknowledge that it will take constant vigilance and dedicated effort to ensure that whistleblowers with claims of retaliation are heard and that their claims are fairly and independently investigated.

Mr. Chairman, this concludes my testimony. I am happy to answer any questions you or other members of the committee may have.