

SPECIAL REPORT

No. 175 | JANUARY 3, 2017

Congress Must Re-Set Department of Homeland Security Priorities: American Lives Depend on It

David Inserra

*Congress Must Re-Set Department of Homeland
Security Priorities: American Lives Depend on It*

David Inserra

About the Author

David Inserra is a Policy Analyst for Homeland Security and Cyber Security in the Douglas and Sarah Allison Center for Foreign and National Security Policy, of the Kathryn and Shelby Cullom Davis Institute for National Security and Foreign Policy, at The Heritage Foundation.

This paper, in its entirety, can be found at:
<http://report.heritage.org/sr175>

The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002
(202) 546-4400 | heritage.org

Nothing written here is to be construed as necessarily reflecting the views of The Heritage Foundation or as an attempt to aid or hinder the passage of any bill before Congress.

Congress Must Re-Set Department of Homeland Security Priorities: American Lives Depend on It

David Inserra

Abstract:

In 2014, the Department of Homeland Security (DHS) had a total budget authority of \$60.4 billion—which grew to \$66.8 billion in 2016. This budget funds a diverse set of agencies that are responsible for a wide range of issues: counterterrorism, transportation security, immigration and border control, cybersecurity, and disaster response. Yet, DHS management of these issues is highly flawed, both in the finer details of its operations and in its broader priorities. Such failure has provoked a small chorus of critics to question the value of DHS as a whole, and whether the U.S. would be better served without it. Serious changes across all of its policy areas, a realignment of its priorities, and reform of the way DHS headquarters operates are imperative to fixing DHS. Heritage Foundation homeland security expert David Inserra details reforms to each major component of DHS with accompanying budget changes.

Executive Summary

The Department of Homeland Security (DHS) needs substantial reform and improvement in order to fulfill its important roles in the areas of security, emergency preparedness and response, and enforcement of immigration laws. This will require changes in nearly every part of DHS, as well as a better prioritization of resources within each of the components and between the components. This executive summary provides key policy recommendations and corresponding budgetary changes for Congress to consider as it moves through the budgetary process.

Department of Homeland Security Total Budget Authority

- DHS Total Budget Authority: approximately *\$64.5 billion*.
- Increasing DHS management funding and strengthening the authority of DHS headquarters in order to improve the coordination, integration, and common situational awareness of DHS components: *\$880 million*.
- Inspector General (IG) unchanged: *\$170 million*.
- Refocusing the Office of Intelligence and Analysis (I&A) on sharing information with state, local, tribal, territorial, foreign, and private-sector partners; streamlining fusion centers; and supporting improved integration of information collected by DHS components: *\$300 million*.
- Supporting increased Customs and Border Protection (CBP) infrastructure and technology and increasing patrols and equipment for CBP officers: *\$13.6 billion*.
- Increasing Immigration and Customs Enforcement's (ICE's) budget to enable expansion of detention and effective alternatives to detention; expanding visa-overstay-removal operations; increasing the number of illegal immigrants removed; and defunding executive actions that weaken immigration enforcement efforts: *\$7 billion*.
- Streamlining the Transportation Security Administration (TSA) to ensure the safe expansion of trusted-traveler programs and private airport screening, and decreasing costs while maintaining security and increasing efficiency: *\$7.5 billion*.
- Expanding Coast Guard funding to support acquisition goals for additional ships and aerial platforms while meeting operational needs: *\$10.85 billion*.
- Increasing Secret Service funding with the need for close oversight during this troubled time in the agency's history: *\$2.2 billion*.
- Strengthening the cybersecurity funding available to the National Protection and Programs Directorate and implementing improved cybersecurity and infrastructure protection policies: *\$3.3 billion*.
- Significantly reforming each of the major parts of the Federal Emergency Management Agency (FEMA), including overhauling the Stafford Act to return responsibility for localized disasters to state and local governments, where they have been handled historically; consolidating and streamlining grants to have a risk-based focus; and fixing the National Flood Insurance Program that is draining U.S. tax dollars: *\$13.5 billion*.
- Reforming U.S. Citizenship and Immigration Services (USCIS) funding to expand fraud prevention in the E-Verify and visa systems while defunding deferred-action memorandums that are unconstitutional and harmful to U.S. immigration law enforcement: *\$3.7 billion*.
- Expanding the Federal Law Enforcement Training Center's operations: *\$300 million*.
- Prioritizing Science and Technology Directorate (S&T) research while encouraging private-sector research and development through the expansion of the Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act: *\$750 million*.
- Maintaining the Domestic Nuclear Detection Office (DNDO) and Office of Health Affairs (OHA): *\$350 million* and *\$130 million*, respectively.

Budget Summary for DHS Management and Inspector General (IG)

Policy Recommendations

- **Create a more unified, standardized procurement and acquisitions process, and a more empowered Chief Procurement Officer,** to drive these reforms.
- **Provide more authority to centralized service components, such as the General Counsel, the Chief Financial Officer (CFO), the Chief Information Officer (CIO), and International Affairs, over their respective component offices.** Such measures should not prevent component heads from exercising their authority, but should ensure that department-level directives are being carried out.
- **Strengthen the DHS Policy Department to develop intra-agency policy, resolve disputes, and drive organizational change that makes DHS components work as a more cohesive unit.**
- **Link policy to planning, budget, and execution.** This requires the development of homeland security doctrine, still lacking 14 years after the department began operation, and a headquarters-led program of Planning, Programming, Budgeting & Execution (PPBE). Most notably, more resources need to be put to the task; from strategic planning to program evaluation, the department systematically underinvests in self-analysis and evaluation.
- **Streamline congressional oversight of DHS.** As the Aspen Institute put it in 2013, “DHS should have an oversight structure that resembles the one governing other critical departments, such as Defense and Justice.” This means placing oversight of DHS under one primary homeland security committee in the House, and one in the Senate, with some additional oversight by the intelligence committees and a homeland security appropriations subcommittee in both chambers.
- **Centralize DHS headquarters.** Without a facility that can accommodate headquarters personnel and relevant component personnel, the integration and synergy of DHS suffers.

Funding

- The Heritage Foundation recommends \$880 million in its proposed budget for departmental management and operations for achieving these recommendations.
- With no serious changes needed to the IG, Heritage recommends \$170 million.

Budget Summary for DHS Intelligence Activities

Policy Recommendations

- **Streamline U.S. fusion centers.** Congress should limit fusion centers to the approximately 30 areas with the greatest level of risk as identified by the Urban Area Security Initiative (UASI). While exceptions might exist, such as certain fusion centers that lead cybersecurity or other important issue-specific efforts, the remaining centers should be fully funded and resourced by the UASI.
- **Refocus DHS's intelligence capabilities.** Intelligence and information is critical to preventing terrorist attacks. Congress should consider redirecting DHS efforts toward information sharing and coordinating proper roles and responsibilities for federal, state, and local counterterrorism measures. Instead of replicating other intelligence efforts, I&A should use the unique data from DHS components.
- **Ensure that the FBI more readily and regularly shares information with state and local law enforcement, treating state and local partners as critical actors in the fight against terrorism.** State and local governments and private-sector partners must send and receive timely information to and from the FBI. DHS should play a role in supporting these partners, by acting as a source or conduit for information and coordinating information sharing between the FBI and its partners.

Funding

- Heritage recommends \$300 million for analysis and operations to carry out these recommendations. Heritage also recommends additional funding for the FBI's National Security and Intelligence branches.

Budget Summary for Customs and Border Protection (CBP)

Policy Recommendations

- **End the 100 percent cargo-scanning mandate.** Congress should reject this cost-inefficient measure and instead support DHS's ongoing efforts to conduct risk-based scanning.
- **End the biometric exit requirement.** Biometric exit is another cost-ineffective solution that does nothing to combat visitors who overstay their visas, and has minimal counterterrorism benefits. Instead, the resources of this program should be spent improving a *biographic* exit system, improving other intelligence tools, and increasing ICE's ability to remove visa overstays.
- **Decouple the Visa Waiver Program (VWP) from the biometric exit requirement.** The VWP enhances U.S. security, trade, and diplomacy and should not be connected to a biometric exit system. Instead, program enhancements to Electronic System for Travel Authorization (ESTA), a modernization of the TECS vetting and investigation management system, and a judicious VWP expansion will make the U.S. more secure and prosperous.
- **Expand Global Entry reciprocity agreements.** The U.S. should build on existing partnerships, not only among nations already participating in Global Entry, but also with VWP member countries, thus creating a trusted-travel superhighway that enhances security and facilitates travel.
- **Improve border security technology and infrastructure.** Improved technology on the border, together with targeted increases in fencing, infrastructure, and other resources for Border Patrol agents, will improve the effectiveness of the CBP.

Funding

- Heritage recommends \$13.6 billion for the CBP.

Budget Summary for Immigration and Customs Enforcement (ICE)

Policy Recommendations

- **Defund the President's executive actions on immigration enforcement.** The Obama Administration has issued a series of policy memorandums that do not allow ICE Enforcement and Removal Operations (ERO) officers to do their jobs. To improve morale and enforce existing immigration laws, Congress should not allow any funding to be used in support of these amnesty and non-enforcement policies. Failing to do so jeopardizes Congress's constitutional authority and sets a dangerous precedent that empowers the executive branch in ways that all Americans should fear.
- **Strengthen the 287(g) program.** Designed to enable state and local government to help enforce federal immigration laws, 287(g) has been under assault during the Obama Administration, which has sought to cut funding, access to, and use of the program. Congress should seek to widen 287(g) usage by increasing funding for the program and requiring DHS to enter into a 287(g) agreement with any state and local governments that requests entry—with significant consequences, should DHS not meet this requirement in a timely fashion.
- **Increase rapid-removal authority.** Currently, Administration policy restricts ICE from removing many illegal border crossers in an expedited manner. To prevent future humanitarian and security crises on the border, ICE should be allowed to rapidly remove any illegal border crosser. This can be accomplished by making this authority explicitly clear in section 235 of the Immigration and Nationality Act of 1952, and by reforming the William Wilberforce Trafficking Victims Protection Reauthorization Act of 2008 to clarify that children who are not victims of human trafficking should also be removed in an expedited manner to discourage future surges.
- **Provide more prosecutors and agents.** In addition to cancelling non-enforcement policies and letting ICE agents do their jobs, Congress should increase the number of ERO officers as well as a corresponding number of prosecutors and legal personnel to increase and expedite removals.
- **Increase the number of immigrants who appear at their court hearings.** While more detention beds mean that more individuals will show up to immigration proceedings, this system can be expensive. Increasing the use of the most effective alternatives to detention (ATD), such as GPS tracking anklets, is a cost-effective way of reducing the number of absconders.

Funding

- Heritage recommends \$7 billion for ICE.
- Heritage also recommends additional funding for Department of Justice immigration judges and support staff.

Budget Summary for the Transportation Security Administration (TSA)

Policy Recommendations

- **Improve security assessments.** In order to continue the judicious growth of TSA PreCheck and risk-based security, the TSA must conduct proper security assessments and refine the screening and vetting process to minimize security risks. Red team exercises should become a larger part of these assessments.
- **Embrace risk-based screening.** Measures, such as the Automated Targeting System, which subject cargo to a risk rating that determines whether it should be given additional screening, are the right way forward in terms of effective air cargo security. Congress and DHS should look for ways to move away from a blanket screening process. At a bare minimum, they should expand the Certified Cargo Security Program, which allows more flexibility in how the private sector may meet the 100 percent screening mandate. Congress and the TSA should also look to expand enrollment in TSA PreCheck to shorten airport security lines.
- **Simplify the Screening Partnership Program (SPP) approval and contracting process.** The process for joining the SPP should be streamlined to make it easier for airports to apply and make TSA adjudication faster, fairer, and more consistent. Airports joining the SPP should also be allowed to select and manage their own screening contractors from a list of TSA-approved companies instead of being micromanaged by the TSA.
- **Limit collective bargaining.** Collective bargaining in the screening line is harming security and costing taxpayers and travelers. Congress should expressly forbid the TSA from bargaining collectively.
- **Expand the Federal Flight Deck Officers (FFDO) program.** Greater funding for the FFDO program will enable this extremely cost-effective program to grow significantly.
- **Review alignment of the TSA budget with the risks.** TSA resources for any given activity should match the relative level of risk that that activity is working to mitigate. This requires that the TSA, its IG, or the Government Accountability Office (GAO) examine classified risk assessments and realign funding to better match the severity of different risks.

Funding

- Heritage recommends \$7.5 billion for the TSA.

Budget Summary for the U.S. Coast Guard (USCG)

Policy Recommendation

- **Recapitalize the U.S. Coast Guard.** Funding for acquiring new Coast Guard vessels has been regularly short of what is necessary to complete the Coast Guard's mission, and often results in additional acquisitions inefficiencies and costs. Congress should commit to providing the Coast Guard with consistent acquisitions funding so that the USCG will have the vessels it needs to complete its missions adequately. Congress should also ensure that any additional resources it provides to the Coast Guard are used to meet important priorities, including cost-efficient acquisition of the Fast Response Cutter (FRC), polar ice breakers, and unmanned systems.

Funding

- Heritage recommends \$10.85 billion to the USCG:
 - **\$1.5 billion for Acquisition, Construction, and Improvements (AC&I).** This funding should include robust Offshore Patrol Cutter (OPC) development, more unmanned aircraft systems, and adequate funding for a cost-effective heavy-duty icebreaker capability.
 - **\$7.06 billion for operating expenses.** Fiscal year (FY) 2016 appropriations included \$7.06 billion for operating expenses, including \$160 million for Overseas Contingency Operations (OCO). The Heritage budget maintains this level of OCO funding for 2017.
 - **The USCG should maintain funding for other programs.** Environmental compliance, reserve training, health care, retirement pay, and other programs are funded at levels requested by the President.

Budget Summary for the U.S. Secret Service (USSS)

Policy Recommendations

- **Increase USSS staffing.** The review panel recommended 85 more Presidential Protective Division (PPD) agents and 200 more officers, but called on the USSS to create a mission-based budget that will determine the appropriate staffing levels.
- **Mandate increased training.** The panel called for PPD agents to spend 25 percent of their on-duty time in training, the so-called Fourth Shift. For the other USSS officers, a minimum of 10 percent training time should be required.
- **Require increased disciplinary and accountability standards.** When improper behavior or mistakes are made, the USSS should demand a strict disciplinary or corrective action. Supervisors and managers must be made to uphold these standards or be made accountable themselves. Congress should require the GAO to report on how these standards are used and whether they are instilling discipline across the service.
- **Expand the number of professional administrators, rather than agents or officers, responsible for budgeting and workforce functions.** The review panel points out that agents and officers may not always be the best at completing administrative tasks, and that a larger suite of professional administrators could support and improve planning and execution of core responsibilities.
- **Provide continued oversight to ensure that reforms are completed thoroughly.**

Funding

- Heritage recommends \$2.2 billion for the USSS.

Budget Summary for the National Protection and Program Directorate (NPPD)

Policy Recommendations

- **Implement cyber-threat and cyber-vulnerability information sharing.** Allowing the private sector and public sector to more easily share information with each other will benefit both sides. By providing strong liability protection for information that is shared, businesses are encouraged to share with the government as well as with other businesses.
- **Help DHS improve and expand its ability to monitor government networks.** The DHS-run “Einstein” intrusion-detection-and-prevention system has grown dramatically over the past decade. With better information sharing, Einstein’s ability to detect and prevent intrusions would be enhanced, but the system must always be improved as the nature of the threats change. DHS needs the clear authority, relationships, and ability to work with other agencies in using Einstein and other cyber tools.
- **Improve morale of DHS staffers.** Morale at the NPPD is incredibly low, which makes it difficult to recruit and keep good employees, especially when private-sector cybersecurity jobs are available. Notably, pay is not the central issue in this survey; the lack of leadership, training, and performance-based rewards are blamed and must be fixed. If DHS is to be an effective actor, it must do more to maintain a highly skilled workforce.
- **Reform risk assessments to capture all relevant information, including consequences, threats, and vulnerabilities.** DHS has a history of conducting risk assessments poorly, and this systemic problem must be resolved. Not correcting this problem means that important security decisions are made with inaccurate information. Trouble with risk assessments at the Federal Protective Service (FPS) and the Infrastructure Security Compliance Division severely hamper the efforts of the NPPD to secure critical infrastructure.
- **Return the Chemical Facility Anti-Terrorism program to a truly risk-based approach.** A risk-based approach would allow chemical facilities and DHS to prioritize their actions and resources to concentrate on threats that pose the most serious risks. This means ensuring that DHS expands the use of Alternative Security Programs, expedites security plan approvals, and improves risk assessments.
- **Improve interoperable communications policies.** The Office of Emergency Communications and coordinating bodies must receive more authority to inject policy into each DHS component. Policies must be improved to ensure that DHS radio users are able to seamlessly communicate with other federal officials, not to mention state and local partners.
- **Explore alternative funding structures for the FPS.** The GAO recommended comparing alternative funding structures to ascertain the pros and cons of different approaches that include some level of direct appropriation. Inserting a more stable source of income might improve the FPS’s budgeting and planning processes as well as improve the way it provides training to its officers. This should be explored by the FPS and the Congressional Research Service.

Funding

- Heritage recommends \$3.3 billion for the NPPD.

Budget Summary for the Federal Emergency Management Agency (FEMA)

Policy Recommendations

- **Reduce the federal share for all FEMA declarations to 25 percent of total cost per declaration.** This way, at least three-fourths of the costs of a disaster are borne by the taxpayers living in the state or states where the disaster took place. For catastrophes with a nationwide or widespread regional impact—such as Hurricane Katrina—a relief provision would provide a higher federal cost share if the total costs of the disaster exceeded an inflation-adjusted threshold.
- **Modify the Stafford Act to establish clear requirements that limit the situations in which FEMA can issue declarations.** One way to do this is to raise the minimum-dollar threshold for requesting disaster declarations. Increasing the per capita threshold to \$3 and properly indexing these sums for inflation would significantly reduce the number of events that would warrant a federal disaster declaration.
- **Consolidate homeland security and emergency-preparedness grant programs and allocate funds in a risk-based manner.** Rather than treating grants as federal dollars to be spread around, federal grant dollars should be focused on the highest-risk areas and issues. As part of this consolidation, grant programs should be evaluated, and ineffective ones—such as Staffing for Adequate Fire & Emergency Response (SAFER), Fire Prevention & Safety (FP&S), and Assistance to Firefighters Grants (AFG)—should be cancelled.
- **Begin to transition nearly all users of the National Flood Insurance Program (NFIP) to private insurance.** The NFIP should be wound down. Within one year, the NFIP should begin ending insurance for lower-risk insured groups, followed by phasing out NFIP insurance for increasingly high-risk properties. Within four years, the NFIP should only exist to serve a select few homeowners who are unable to acquire

insurance, not because the cost is too high, but because it is not offered where they live. These properties, however, should pay a rate that is as actuarially fair as possible.

Funding

- Heritage recommends \$13.5 billion for FEMA.

Budget Summary for U.S. Citizenship and Immigration Services (USCIS)

Policy Recommendations

- **Reject political influence in the visa-adjudication process.** When executive policymaking forces USCIS employees to cut corners, and high-ranking politicians are able to wield their influence to obtain green cards for their friends and businesses, the U.S. effectively has a two-tier immigration system—one that serves the well-connected and special interests, and one that deals with everyone else. Good governance requires that this sort of corruption end. Congress should require the Inspector General to conduct ongoing investigations into the way political influences are pressuring USCIS employees to bend the rules.
- **Restart comprehensive immigration-fraud evaluations.** The U.S. is a generous nation that provides many people with immigration benefits, but there are many who abuse the system. Given the value of U.S. visas and citizenship, the U.S. should do more to investigate fraud, both on a case-by-case basis, and through more complete assessments and investigations.
- **Strengthen E-Verify against identity theft.** E-Verify prevents unauthorized individuals from being hired, but one flaw of the system is that those who use legitimate Social Security numbers acquired through identity theft can be authorized. The Social Security Administration should be required to work with the E-Verify system to identify cases where Social Security numbers are being used in multiple places or in suspicious ways.
- **Reform the USCIS's funding mechanism.** To help the USCIS conduct more fraud prevention, acquire better IT systems such as the Electronic Immigration System, and improve other administrative functions, the USCIS funding model should be changed. Currently, only E-Verify is funded by appropriations. Congress should move administrative parts of the agency to more regular appropriations to ensure that basic functions are not funded according to visa revenues.
- **Ensure refugee resettlement is secure.** Congress should continuously demand risk assessments regarding the resettlement of refugees and how the administration is managing that risk. Congress should also push USCIS to enhance the training and expertise of USCIS refugee officers as well as updating and improving DHS's vetting and immigration systems.
- **Promote real assimilation.** Becoming an American should be a meaningful experience that instills immigrants with a love of America and her values. Current integration efforts portray citizenship as little more than a right to a U.S. passport. The USCIS must retool its integration measures, and, instead of emphasizing multiculturalism, diversity, and political activism as the desired values, promote patriotism, American principles, and civic education.

Funding

- Heritage recommends \$3.7 billion for the USCIS.

Budget Summary for the Federal Law Enforcement Training Center (FLETC)

Policy Recommendations

- **Expand training for state and local law enforcement.** Since state and local law enforcement officers are often the first to respond and deal with a crisis, such as an active shooter, DHS should expand “train the trainer” programs and direct training of state and local officers.
- **Consolidate training facilities under the FLETC.** DHS should act on multiple studies recommending ways to consolidate additional facilities into the FLETC. As part of that consolidation, Congress should require a study to see if other training facilities planned for or operated by other agencies could be consolidated and operated by the FLETC.

Funding

- Heritage recommends \$300 million for law enforcement training.

Budget Summary for DHS Research and Development (R&D) Organizations

Policy Recommendations

- **Develop clear policies for overseeing R&D.** With S&T only recently defining what R&D is, S&T and other DHS components must properly report and account for spending on their research activities. This should feed into a mechanism for tracking R&D projects and total expenditures. While S&T has taken preliminary steps to assign roles and responsibilities for coordination of R&D projects, Congress should oversee these new guidelines to ensure that relevant agencies are fulfilling their responsibilities.
- **Reject inserting pork into R&D missions.** R&D is a common area in which Congress mandates certain pork-barrel projects that benefit parochial interests in Members' districts regardless of the wisdom of such an investment. While Congress can and should oversee spending, it should not insert political and parochial interests to the detriment of R&D.
- **Focus on primary customers—DHS components.** While S&T's efforts can have benefits for state, local, and private-sector needs, S&T should focus on meeting the needs of DHS components first and foremost.
- **Formalize relationships between S&T and other components.** To better coordinate research and meet component needs, Congress should more formally connect S&T with research and requirement-setting activities. At a high level, this means the creation of a formal oversight council or process to ensure that S&T and relevant parties share visibility and understanding of research projects. At a lower level, this means expanding initiatives, such as Apex programs, which involve integrating component staff in the S&T R&D process to increase research usefulness to end users.
- **Expand the SAFETY Act.** One way to support the development of products that support end-user needs is to expand the Support

Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act, as profit is a good incentive for developing products and services that meet user needs. By expanding the SAFETY Act's protections in a reciprocal nature with other nations, the U.S. will have access to even more lifesaving technologies. Congress should start a pilot program with a willing ally, such as Israel, to work out the details.

Funding

- Heritage recommends:
 - \$750 million to S&T.
 - \$350 million for the DNDO.
 - \$130 million for the OHA.

TABLE 1

Actual and Suggested Budget for the Department of Homeland Security

FIGURES IN THOUSANDS			
Agency	Enacted* FY 2016	President's Request FY 2017	Heritage Budget FY 2017
Departmental Management and Operations	\$1,069,328	\$1,011,511	\$880,000
Analysis and Operations	\$264,714	\$265,719	\$300,000
Office of the Inspector General (includes \$24 million from FEMA)	\$161,488	\$181,144	\$170,000
U.S. Customs and Border Protection	\$13,254,127	\$13,940,997	\$13,600,000
U.S. Immigration and Customs Enforcement	\$6,154,041	\$6,230,206	\$7,000,000
Transportation Security Administration	\$7,440,096	\$7,589,079	\$7,500,000
U.S. Coast Guard**	\$11,112,251	\$10,321,548	\$10,850,000
U.S. Secret Service	\$2,198,545	\$2,156,119	\$2,200,000
National Protection and Programs Directorate	\$3,079,054	\$3,044,846	\$3,300,000
Office of Health Affairs	\$125,369	Into CBRNE	\$130,000
Federal Emergency Management Agency	\$16,574,971	\$16,539,803	\$13,500,000
U.S. Citizenship and Immigration Services (USCIS)***	\$3,610,217	\$4,018,270	\$3,700,000
Federal Law Enforcement Training Center	\$245,038	\$242,518	\$300,000
Science and Technology Directorate	\$786,938	\$758,743	\$750,000
Domestic Nuclear Detection Office	\$347,120	Into CBRNE	\$350,000
CBRNE (Chemical, Biological, Radiological, Nuclear, and Explosives)		\$501,445	
Totals	\$66,423,297	\$66,801,948	\$64,530,000

* Figures are drawn from Public Law 114-113, Explanatory Statement of Chairman Rogers, and President Obama's budget request materials.

** Figures are for FY 2016 and include approximately \$160 million in OCO funding and a rescission of \$32.4 million, resulting in a figure about \$127.5 million higher than stated in some budget documents.

*** Figures are estimates. Since USCIS is largely funded by fees, it will remain unclear how much was spent until after the fiscal year ends.

SOURCES: Consolidated Appropriations Act, 2016, Public Law 114-113, <https://www.congress.gov/bill/114th-congress/house-bill/2029/text> (accessed April, 2016); "Explanatory Statement Submitted by Mr. Rogers of Kentucky, Chairman of the House Committee on Appropriations, Regarding Division F, the "Department of Homeland Security Appropriations Act, 2016," H.R. 2029, "Consolidated Appropriations Act, 2016," U.S. House of Representatives, <http://docs.house.gov/meetings/RU/RU00/20151216/104298/HMTG-114-RU00-20151216-SD007.pdf> (accessed April 12, 2015); U.S. Department of Homeland Security, "Congressional Budget Justification, FY 2017," <https://www.dhs.gov/publication/congressional-budget-justification-fy-2017> (accessed April 12, 2016); and U.S. Department of Homeland Security, "Budget-in-Brief, Fiscal Year 2017," <https://www.dhs.gov/sites/default/files/publications/FY2017BIB.pdf> (accessed April 12, 2016).

In 2015, the Department of Homeland Security (DHS) had a total budget authority of \$63.5 billion—which grew to \$66.3 billion in 2016.¹ This budget funds a diverse set of agencies responsible for a wide range of issues: counterterrorism, transportation security, immigration and border control, cybersecurity, and disaster response. Yet, DHS’s management of these issues is highly flawed, both in the finer details of its operations and its broader priorities. Such failure has provoked a small chorus to question the value of DHS as a whole and whether the U.S. would be better served without it. Serious changes across all of its policy areas, a realignment of its priorities, and reform of the way DHS headquarters operates are imperative to fixing DHS.

Through the budgeting process, Congress has legislative authority to reform DHS. It can and should use its budgetary authority to expand some programs, alter others, and shrink or defund those programs that are flawed, inefficient, or low priorities. DHS does not need more funding—it needs better prioritization of its funding. The Heritage Foundation has constructed a complete reform agenda and an alternative, \$64.5 billion budget that proposes:

- **Increasing** DHS management funding and strengthening the authority of DHS headquarters to improve the coordination and integration of all DHS components;
- **Refocusing** the Office of Intelligence and Analysis on sharing information with state, local, tribal, territorial, foreign, and private-sector partners; streamlining fusion centers; and supporting improved analysis and integration of information collected by DHS components;
- **Supporting** increased Customs and Border Protection (CBP) infrastructure and technology; increasing patrols and equipment for CBP officers; and updating the CBP’s information-sharing system, TECS;
- **Increasing** the budget of Immigration and Customs Enforcement (ICE) to enable expansion of detention and effective alternatives to detention; expanding visa-overstay-removal operations; increasing the number of illegal immigrants who are removed; and defunding executive actions that weaken immigration enforcement;
- **Streamlining** the Transportation Security Administration (TSA) to ensure the safe expansion of trusted-traveler programs and private airport screening, decreasing costs while maintaining security and increasing efficiency;
- **Expanding** Coast Guard funding to support acquisition goals for additional ships and aerial platforms;
- **Increasing** Secret Service funding and training, with emphasis on better oversight during this troubled time in the agency’s history;
- **Increasing** the cybersecurity funding for the National Protection and Programs Directorate (NPPD), and implementing improved cybersecurity and infrastructure-protection policies;
- **Significantly reforming** each of the major parts of the Federal Emergency Management Agency (FEMA), including overhauling the Stafford Act to return responsibility for localized disasters to state and local governments, where they have historically been handled; consolidating and streamlining grants toward a risk-based focus; and reforming the National Flood Insurance Program (NFIP) that is draining U.S. tax dollars;
- **Reforming** U.S. Citizenship and Immigration Services (USCIS) funding to expand fraud prevention efforts in the E-Verify and visa systems while defunding deferred-action policies that are unconstitutional and harmful to U.S. immigration law enforcement;
- **Expanding** the Federal Law Enforcement Training Center’s (FLETC’s) operations and availability; and
- **Prioritizing** Science and Technology Directorate (S&T) research while encouraging private-sector research and development through the expansion of the Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act of 2002.

While Congress may be hesitant to flex its budgetary muscles after surrendering to the executive branch on a DHS continuing resolution for fiscal

year (FY) 2015, Congress must use this power, or else become a mere rubber stamp for executive action or inaction, not to mention continued program and policy problems and failures. U.S. security and safety, the rule of law, and limits on the executive are all at stake in the budgeting process, and it is past time that the first branch of government exercise its constitutional authority to make major reforms to DHS.

1. Management

DHS management and headquarters received a significant increase in FY 2016, from around \$743 million in FY 2015 to \$1.12 billion in the FY 2016 appropriation. This increase includes several large sums from the general provisions section of the DHS appropriations, including \$50 million for counterterrorism funding, \$100 million for improving DHS cybersecurity systems and capabilities, \$53 million for modernizing the financial system, and \$216 million to build the new DHS headquarters building.² This funding increase is not entirely uncalled for. DHS faces a number of challenges that it has yet to adequately address. DHS has been given a difficult mission and it has not yet been able to achieve the synergies required to carry out that mission. A key reason for this is DHS's failure to fully integrate its management structure. The Government Accountability Office (GAO) has characterized the Homeland Security Department this way:

The Department of Homeland Security's (DHS) efforts to strengthen and integrate its management functions have resulted in it meeting three and partially meeting two of GAO's criteria for removal from the high-risk list.... However, DHS needs to show additional results in other areas, including demonstrating the ability to achieve sustained progress across 30 outcomes that GAO identified and DHS agreed were needed to address the high-risk area. As of March 2016, DHS had fully addressed 10 of these outcomes but work remained in 20.³

In DHS's management of acquisitions, the GAO found that while component acquisition capabilities were improved, major concerns remain over the number of trained acquisition personnel at headquarters and component levels, and the ability to determine "that major acquisition programs are on

track to achieve their cost, schedule, and capability goals."⁴ The GAO also reported serious problems with DHS financial management, finding serious deficiencies in departmental and component financial management systems despite recent improvements. The GAO described these problems as representing "long-term challenges in obtaining and sustaining a clean audit opinion on internal control over financial reporting, and ensuring its financial management systems generate reliable, useful, and timely information for day-to-day decision making."⁵ The GAO also found problems in DHS's management of information technology and technology integration, including problematic component-level adoption of some elements of headquarters' IT plans, information security, headquarters' financial-reporting systems, and the need for sustained progress in its integration of management efforts across the department.

The GAO report also described widespread human capital and morale issues that plague the department. The Office of Personnel Management's (OPM's) 2014 Federal Employee Viewpoint Survey "showed that DHS's scores continued to decrease in all four dimensions of the survey's index for human capital accountability and assessment—job satisfaction, talent management, leadership and knowledge management, and results-oriented performance culture."⁶ The 2015 survey showed that DHS continued its decline across the board, a four-year downward trend for the department.⁷ According to the yearly survey conducted by the Partnership for Public Service, DHS is currently the worst large agency in the federal government for which to work—far worse than the second-worst agency, the scandal-ridden Department of Veterans Affairs.⁸ Seven of the 10-lowest-ranked subcomponents for which to work are within DHS. The Office of the Secretary and the Management Directorate score at 283 and 306, respectively, out of 320 agency subcomponents. These organizations do not all have morale problems by coincidence—the mismanagement of DHS is causing the department to suffer. Fourteen years after the creation of DHS, excuses must stop, and serious improvement must start.

DHS management issues, however, cannot be entirely blamed on DHS. The labyrinthine web of congressional oversight of DHS is sucking up DHS's time and resources and providing duplicative or contradictory oversight. There is bipartisan agreement

amongst former and current DHS officials, think tanks, and the 9/11 Commission that the current byzantine system of congressional oversight of DHS is harming security due to power politics.⁹ There is no reason for jurisdiction over DHS to be split across about 100 committees and caucuses other than congressional Members' unwillingness to give up a small slice of their power in exchange for improved security and efficiency. There is no disagreement on this matter. And so the chorus of experts continues to beg Congress to do the right thing and finally put security before politics.

Actions for Congress. Building on the recommendations of the GAO and others, Congress should undertake non-flashy, but important, reforms of DHS management systems and processes. Congress should:

- **Create a more unified, standardized procurement and acquisitions process, and empower the Chief Procurement Officer to drive these reforms.**
- **Provide more authority to centralized service components, such as the General Counsel, the Chief Financial Officer (CFO), the Chief Information Officer (CIO), and International Affairs, over their respective component offices.** Such measures should not exclude component heads from exercising their authority, while ensuring that department-level directives are being carried out.
- **Strengthen the DHS Policy Department to develop intra-agency policy, resolve disputes, and drive organizational change that makes DHS components work as a more cohesive unit.**
- **Link policy to planning, budget, and execution.** Such linking requires the development of homeland security doctrine, still lacking more than 14 years after the department began operation, and a headquarters-led program of Planning, Programming, Budgeting & Execution (PPBE). Most notably, more resources need to be put to the task; from strategic planning to program evaluation, the department systematically under-invests in self-analysis and evaluation.

- **Streamline congressional oversight of DHS.** As the Aspen Institute put it in 2013, "DHS should have an oversight structure that resembles the one governing other critical departments, such as Defense and Justice."¹⁰ This means placing oversight of DHS under one primary homeland security committee in the House and the Senate with some additional oversight by the Intelligence Committees and a homeland security appropriations subcommittee in both chambers.¹¹

- **Centralize DHS headquarters.** Without a facility able to accommodate headquarters personnel and relevant component personnel, the integration and synergy of DHS suffers.

To fund these activities, The Heritage Foundation recommends \$880 million.

Analysis and Operations

With \$252 million in FY 2015 and \$265 million in FY 2016, President Obama requested \$265 million again in FY 2017 for Analysis and Operations activities. Many details concerning Analysis and Operations are classified and receive National Intelligence Program (NIP) funding. Created after 9/11, DHS's *raison d'être* was to better prepare the U.S. for combating terrorism. To this end, DHS, in addition to components such as the CBP, began to analyze and use information to prevent threats to the U.S. before they materialize. Thus, the Office of Intelligence and Analysis (I&A) and the Office of Operations Coordination (OPS) were created. DHS, however, was not to become a full-fledged domestically focused intelligence organization, with the FBI given that responsibility instead after 9/11. As a result, DHS's role in the intelligence arena remains limited. It does, however, have unique access to a variety of travel and immigration information, which it can provide to other agencies.

The nature of the terrorist threat has changed over time and grown more serious. With the rise of ISIS and other Islamist groups in Syria, the U.S. has seen a dramatic increase in terrorist activity at home. In 2015, the U.S. faced 17 Islamist terror plots and attacks, more than any other year since 9/11. At the time of this writing, the U.S. already had 12 terror plots and attacks in 2016, bringing the total to 93 since 9/11. FBI Director James Comey agrees that, given the escalation of foreign fighters and those who seek to join a radical Islamist group in Syria, the U.S. is facing more

terrorist threats to the homeland now than any time since 9/11,¹² a sentiment echoed by other leading intelligence and law enforcement officials.¹³

Given this threat, it is critical that the U.S. make the most of its counterterrorism resources. In 2012, the Senate Homeland Security and Government Affairs Committee found that fusion centers “often produced irrelevant, useless or inappropriate intelligence reporting to DHS and many produced no intelligence reporting whatsoever.” It also provided multiple assessments and examples that show that fusion centers are not meaningfully contributing to counterterrorism measures and may have even been harming them.¹⁴ A more recent report by the RAND Corporation also found that fusion centers have mixed results and often serve different purposes.¹⁵ Meant to serve as hubs of cooperation between federal, state, and local officials, 78 fusion centers often serve cities or regions already covered by 104 FBI Joint Terrorism Task Forces (JTTFs) and 56 Field Intelligence Groups (FIGs), which play a similar role to that of fusion centers.¹⁶ This broad duplication of efforts results in an inefficient and counterproductive use of counterterrorism funds.

In 2013, the DHS Inspector General (IG) reported that DHS’s Homeland Security Information Network (HSIN)—designed to share sensitive but not classified information with federal, state, and local governments and private-sector partners—was only being used by a small percentage of all potential partners. State and local officials stated that one reason for not using the HSIN was that “the system content was not useful.”¹⁷ Since the IG report came out, however, the HSIN has successfully migrated to an updated system and is seeking to add desired content from DHS components and attract more users. At around 36,000 active users at the end of 2014, the HSIN is far short of an Office of Management and Budget target for 2015 of 130,000 users. However, since the move to the new HSIN system, this seems to have improved, with 65 percent of respondents in 2014 saying that HSIN met their needs at least most of the time, with 83 percent of respondents using HSIN at least weekly.¹⁸

I&A also faces other challenges, such as with its workforce. A 2014 GAO report found that I&A was slower in hiring applicants than other agencies in the intelligence community, harming DHS’s ability to attract talent. The GAO noted that this has resulted in a “reliance on contractors to fill the gaps in Intelligence Community experience.”¹⁹ The GAO

also noted I&A’s professional development challenges and high levels of attrition in its workforce. Such difficulties have certainly helped cause, and have been caused, by low morale, as I&A was rated the worst office for which to work in the federal government in 2015.²⁰

Actions for Congress. To better protect the U.S. from terrorism, Congress should:

- **Streamline U.S. fusion centers.** Congress should limit fusion centers to the 28 areas with the greatest level of risk as identified by the Urban Area Security Initiative (UASI).²¹ Some exceptions might exist, such as certain fusion centers that are leading cybersecurity or other important topical efforts. These centers should then be fully funded and resourced by the UASI.
- **Refocus DHS’s intelligence capabilities.** Intelligence and information is critical to preventing terrorist attacks. Congress should consider redirecting DHS efforts toward information sharing and coordinating proper roles and responsibilities for federal, state, and local counterterrorism. Instead of replicating other intelligence efforts, I&A should also focus on using its unique data from DHS components.
- **Ensure that the FBI more readily and regularly shares information with state and local law enforcement, treating state and local partners as critical actors in the fight against terrorism.** State and local governments and private-sector partners must send and receive timely information from the FBI. DHS should play a role in supporting these partners’ efforts by acting as a source or conduit for information between partners and coordinating information sharing between the FBI and its partners.

To fund these activities, the Heritage budget recommends \$300 million for analysis and operations. Heritage also recommends additional funding for the FBI’s National Security and Intelligence branches.

2. Inspector General

For FY 2016, approximately \$161 million was budgeted for the Inspector General. President Obama’s FY 2017 budget requested \$181 million. With no serious changes needed to the IG, Heritage recommends \$170 million.

3. Customs and Border Protection

Approximately \$13.25 billion was budgeted in FY 2016 for CBP; President Obama requested \$13.94 billion for FY 2017. CBP is the largest DHS component by budget and full-time workers. Its primary activities consist of security and inspection of travelers and goods at U.S. ports of entry (POE), including seaports, airports, and land-border crossings, as well as border security between those POEs. While CBP could use targeted investments, the U.S. should not throw away fiscal discipline.

At POEs, CBP currently struggles with several unwieldy mandates, including a requirement to scan 100 percent of containers arriving in the U.S. by sea, and a biometric exit mandate for visitors to the U.S. The scanning requirement means that 100 percent of sea cargo bound for the U.S. has to be scanned by radiation detection and imaging technologies before being sent to the U.S.²² This mandate has been delayed twice due to cost and technology concerns that seem insurmountable. Indeed, the most recent information from CBP in 2011 indicated that only 1 percent of cargo was scanned overseas and another 4 percent was scanned here in the U.S.²³ Even if the money and technology did exist, funding spent on 100 percent scanning could be better spent on intelligence tools that ascertain which cargo shipment is high risk, and subjecting that cargo to additional scrutiny and scanning. Full implementation of the scanning mandate will not only entail costs for CBP, but would also entail delays and costs to the global supply chain, foreign nations, and U.S. consumers, since more than 10 million containers enter the U.S. every year.²⁴

On the other hand, the 100 percent biometric exit requirement is focused on visitors leaving the United States. Currently, the U.S. *accepts* biometric (fingerprint) and biographic (names) information for inbound visitors and uses that data to cross-check against various terror, law-enforcement, and immigration watch lists and systems. The U.S., however, has *only* a biographic exit system, despite a requirement for a biometric exit system since the Intelligence Reform and Terrorism Prevention Act of 2004. Once again, technology, cost, and logistics concerns have made the implementation of such a system difficult at airports, not to mention the statutory requirement for use at all POEs including sea ports and land ports.²⁵ While a biometric exit system may be slightly more accurate and helpful than

a biographic one, it is not currently cost-effective in combatting illegal immigration or terrorism—the dollars spent on a biometric exit system would be better spent improving the biographic system and increasing immigration enforcement and intelligence capabilities.

The biometric exit mandate is also a road block to the expansion of the Visa Waiver Program (VWP), which enhances security and promotes travel. The VWP allows residents of member countries to visit the U.S. without a visa for up to 90 days in exchange for security cooperation and information sharing, and reciprocal travel privileges for U.S. residents. With more intelligence, the U.S. is better able to stop bad actors and terrorists, and it allows the existing visa process to focus its consular and visa resources on those individuals about whom less is known and those who are higher risks to U.S. security.²⁶ Despite unfounded security concerns, the VWP screens individuals through multiple systems, such as its TECS system that queries multiple security databases, including the Terrorist Screening Database.

Indeed, following the terrorist attacks in San Bernardino and Paris, Congress added various restrictions to the VWP, including denying VWP status to those who had visited certain countries (Iraq, Iran, Syria, or Sudan), or who hold dual citizenship in one of these countries. While some of the other steps regarding e-passports and expanded cooperation with other countries on airport and travel security were good additions, the additional restrictions do little to mitigate the risks of terrorism. For example, dual citizenship is a weak indicator of risk, considering that some countries, such as Iran, do not let their citizens forfeit citizenship, even if they received citizenship through their emigrated parents and have never so much as visited Iran. Furthermore, for DHS to stop such dual citizens from using the VWP, it relies on those same individuals to self-report their dual citizenship on the Electronic System for Travel Authorization (ESTA) application—something about which a knowledgeable terrorist or criminal would simply lie. Instead, this provision has had, and will have, harmful side effects for aid workers, journalists, businessmen, and dissidents and their children. Similarly, using travel to Syria as a disqualifier for using the VWP punishes those whose travel the U.S. knows about, but does nothing to stop a terrorist who snuck into Syria and, since his travel was undetected, is still allowed to use the VWP.

Expansion of this program has been extremely limited due to linking the biometric exit mandate to VWP expansion. These two programs should be unlinked, and Congress should remove the biometric exit requirement.

CBP also manages several trusted-traveler programs²⁷ that require a background check and include PreCheck benefits for U.S. citizens and permanent residents; these programs also provide expedited immigration and customs processing at airports or land borders, depending on the specific program.²⁸ The Global Entry program is open to U.S. citizens and permanent residents as well as citizens from six other nations, including Germany and South Korea, which allow U.S. citizens to join an equivalent program. The NEXUS program provides U.S. and Canadian citizens and residents with expedited processing when travelling between the two countries, while the SENTRI program expedites processing through land ports of entry on the southern U.S. border.²⁹ Reciprocal agreements, such as those through Global Entry, should be expanded to provide both the U.S. and its allies with the security and convenience of trusted-traveler programs.³⁰

CBP's other major duty is border security, carried out by the Border Patrol. During the summer of 2014, a surge of children and families from El Salvador, Honduras, and Guatemala stretched DHS resources, including CBP's. The failure of successive Administrations to secure the border and enforce immigration laws have come to a head under President Obama, creating an incentive for yet more illegal immigration from the south. Together with widespread poverty and violence in these Northern Triangle countries, last summer was a perfect storm of events leading to a border crisis. The Obama Administration responded by allowing most families and children to remain in the U.S., sending them to various destinations across the U.S. to await full immigration proceedings. Rather than use its authority to rapidly return recent illegal border crossers to their home countries, as allowed under section 235 of the Immigration and Nationality Act, the Administration's response resulted in additional costs across the immigration system.³¹ Furthermore, the near complete failure to enforce U.S. immigration laws, as described in the "Immigration and Customs Enforcement" and "U.S. Citizenship and Immigration Services" sections below, is only encouraging additional illegal immigration, which makes the

Border Patrol's job that much more difficult. An increasingly difficult job beset by the policies adopted by organizational leaders and the President are cutting into organizational morale, with CBP dropping to 314 of 320 subcomponents in 2015 surveys on employee morale.³²

Additional resources should be focused on improving the infrastructure, resources, and technology available to CBP to apprehend illegal immigrants and prevent entry of those who could pose a risk to the U.S.

One infrastructure improvement would be more secure fences along the southern border.³³ In 2006, President George W. Bush signed into law the Secure Fence Act, which called for approximately 700 miles of new fencing along the southern border.³⁴ DHS has put up the fencing, but the majority of it does not stop foot traffic, with much of the fencing being anti-vehicle "fencing" that is little more than metal poles or bars sunk into the ground every few feet. While some discretion in deciding what kind of fencing to use is appropriate, the U.S. would have a more secure border if double-layered fencing was installed to prevent pedestrian border crossers, as envisioned by the Secure Fence Act. These fences would be especially helpful in areas with a U.S. city or suburb on the other side of the border, which make it easy for illegal border crossers to fade into the background. But in addition to fences, facilities for processing incoming travelers, adjudicating immigration claims, and other customs and immigration tasks should also be considered.

While fences are important, they are far from a silver bullet—there are always alternative ways to entering and remaining in the country illegally. Increasing the amount of technology and wide-area surveillance technology available to the Border Patrol can make it more effective at finding and stopping border crossers. While past programs, such as the Secure Border Initiative Network (SBI-net), have had technical problems, the concept—a network of surveillance technologies to watch the border—is a sound one. Rather than reinventing the wheel, DHS should borrow from the experiences and technologies of the U.S. military and its need for persistent, wide-area surveillance technologies in Iraq and Afghanistan. These systems are already in production, and using and adapting these systems would allow DHS to avoid the expensive development of new systems. With troops and their systems

returning home, DHS may even be able to make use of surplus systems that the military does not need. The military would likely be able to provide training and support to DHS in setting up and operating these systems.

Actions for Congress. To improve U.S. efforts to protect the U.S. border and facilitate trade and travel without sacrificing security, Congress should make the following reforms to CBP:

- **End the 100 percent cargo-scanning mandate.** Congress should reject this cost-inefficient measure and instead support DHS's ongoing risk-based scanning programs, focusing scanning resources on cargo that is considered highest-risk.
- **End the biometric exit requirement.** Biometric exit is another cost-ineffective solution that does nothing to stop visitors who overstay their visas. While biometric exit has minimal counterterrorism benefits, the resources that would be spent on this program should be spent on improving a biographic exit system, improving other intelligence tools, and increasing ICE's ability to remove visa overstayers.
- **Decouple the Visa Waiver Program (VWP) from the biometric exit requirement.** The VWP enhances U.S. security, trade, and diplomacy and should not be connected to a biometric exit system. Instead, program enhancements to the Electronic System for Travel Authorization (ESTA), a modernization of the TECS vetting and immigration system, and a judicious VWP expansion will make the U.S. more secure and prosperous.
- **Expand Global Entry reciprocity agreements.** The U.S. should build on existing partnerships, not only with nations already participating in Global Entry, but also with VWP member countries, thus creating a trusted-traveler superhighway that enhances security and facilitates travel.
- **Improve border security technology and infrastructure.** Improved technology on the border, together with targeted increases in fencing and other resources for Border Patrol agents, will improve the effectiveness of the Border Patrol.

To fund these activities, the Heritage budget recommends \$13.6 billion for CPB.

4. Immigration and Customs Enforcement

One of the most troubled agencies throughout the U.S. government, ICE had a budget of around \$6.15 billion in FY 2016, and the President's FY 2017 request would give ICE \$6.23 billion in total budget authority. In addition to greater funding, ICE is in desperate need of major policy changes to boost morale and effectiveness.

Composed of two field divisions, Homeland Security Investigations (HSI) and Enforcement and Removal Operations (ERO), as well as Management and Administration and the Office of the Principal Legal Advisor, HSI and ERO maintain largely separate priorities. HSI focuses on combatting transnational crime and trafficking, international visa security, countering fraud operations, customs and intellectual property rights enforcement, and antiquities and art operations. As an organization more closely resembling traditional criminal law enforcement, HSI is largely free to pursue these goals. ERO, on other hand, is intended to focus on removing illegal immigrants, as well as legal immigrants and temporary workers who have committed a crime or are removable for another reason. ERO, however, is largely forbidden from pursuing the very objective for which it is intended. Numerous policies and pressures are placed on ICE agents to prevent them from enforcing the law. Ranging from the Morton Memos in 2011³⁵ to the Deferred Action for Childhood Arrivals Program, to enforcement "priorities" and the Deferred Action for Parents of Americans (DAPA) in the President's executive action, ICE agents have been ordered to avoid enforcing the law against almost all illegal immigrants other than the most serious criminals.³⁶ The result is that once an individual overstays a visa or makes it past the border, it is unlikely that ICE will ever find or enforce the law against him.

Indeed, deportations of individuals from the U.S. interior have cratered in the past several years. DHS statistics indicate that the U.S. conducted only 462,463 removals and returns, known to the average American as deportations, in FY 2015, plummeting to their lowest level since 1971.³⁷ Deportations from the interior of the U.S. dropped from around 230,000 in FY 2010 to approximately 70,000 in FY 2015, a decline of 70 percent in just five years.³⁸ Even

though removing criminal aliens is an Administration “priority,” ICE deported just over 63,000 criminal aliens from the U.S. interior in 2015, a decline of almost 60 percent from the 150,000 deported in FY 2011.³⁹ With deportations falling further, ICE is set to break more historical records on how few illegal immigrants it can deport.

The consequence of such action is that in the Partnership for Public Service’s 2014 annual survey, ICE was rated the worst organization in the federal government for which to work, with a steady downward trend since 2010 that corresponds with the Obama Administration’s actions on immigration. In 2015, ICE’s score fell further, but other DHS subcomponents fell even more, making ICE the third-worst place to work in the federal government.⁴⁰ There are few things more disheartening than signing up for a job and being dedicated to its mission and then not being allowed to do it. This is precisely the position in which ICE officers, especially in ERO, find themselves.

Furthermore, many foreigners who are in the U.S. illegally do not appear at their own court hearings for their deportation proceedings. According to the Department of Justice’s Executive Office of Immigration Review, 34 percent of non-detained aliens (illegal or legal) absconded from the court in FY 2014, rising to 43 percent in FY 2015.⁴¹ Testimony by Brandon Judd, president of the National Border Patrol Council, which represents 18,000 Border Patrol agents, recently testified that DHS policy now requires Border Patrol agents to release, without any notice to appear in court, anyone they catch who has not been convicted of a felony so long as he claims to have been in the U.S. since January 2014.⁴² Such “catch and release” policies further undermine the enforcement of U.S. immigration laws and artificially deflate the absentia rates by never including deportable aliens in the immigration process to begin with. If the U.S. is serious about stopping those who abscond, it should seek to increase the number of detention beds available, increase the use of effective alternatives to detentions (ATD) including GPS tracking anklets, and do more to ensure that ICE and DOJ immigration officials have—and use—the resources and tools to more rapidly remove illegal border crossers and visa overstayers.

The Obama Administration has also crippled state and local enforcement of immigration laws. Despite the importance of federalism to the U.S.,

the Obama Administration has attacked states that have taken action that comports with the letter and intent of federal immigration law. Utah, South Carolina, Alabama, and, most notably, Arizona, have all passed immigration laws that attempt to allow state and local officials to check the immigration status of individuals stopped in the due course of lawful police actions, and otherwise help federal authorities enforce U.S. immigration laws.

In a case ultimately argued before the Supreme Court, the U.S. government asserted that federal enforcement policies pre-empted Arizona’s 2010 immigration law, S.B. 1070, despite the fact that Arizona’s law was *based on* federal law. The U.S. government argued that its enforcement priorities and policies were the supreme law and that even if they deviated from the clear meaning and letter of the law, states had no right to enforce federal law since such enforcement deviated from the federal government’s policies.⁴³ This line of argument turns jurisprudence on its head, as it establishes not the law, but any given Administration’s preference as the supreme law of the land—dangerous territory for a nation that depends on the rule of law.

Five justices at least partially agreed with such a notion. While the Supreme Court upheld the vast majority of S.B. 1070, the court did reject three measures despite their clear basis in federal law. The Supreme Court did, however, affirm that states have an important role to play in enforcing federal immigration law: The court confirmed the ability of states to pass laws like S.B. 1070 that make it a state crime to engage in human smuggling, to hire illegal day-laborers on the roadside, or to encourage an individual to illegally cross the border, as well as requiring state law enforcement officers to check the immigration status of anyone they stop or detain where there is reasonable suspicion that the person might be in the country illegally.⁴⁴

States like Arizona, which are experiencing significant problems with illegal immigration, or that are frustrated by the federal government’s lack of enforcement, are trying to step up and assist in enforcing immigration law. Just as state and local law enforcement resources should be and are used to combat terrorism due to the amount of state and local resources scattered across the U.S., so, too, should state and local government be partners in enforcing immigration law. With approximately 1.2 million state and local law enforcement officers and

staff serving across the nation, the U.S. would be foolish to not take advantage of their local knowledge and presence.

Congress has created multiple programs that make use of local law enforcement, including the 287(g) program, Operation Stonegarden grants, and the Border Enforcement Security Task Force (BEST) units. Each of these programs serves an important purpose and, together with independent state efforts, helps to enforce U.S. immigration law more effectively. The Obama Administration has consistently rejected, cut funding for, fought, or limited many of these cooperative programs and state efforts. A central tenet of the Obama Administration has been to centralize power within the federal government, and nowhere is this truer than in immigration policy, where the executive branch has argued that it alone can enforce, or refuse to enforce, federal law. State and local officials are willing to volunteer to be trained to help enforce federal immigration law, but the executive branch has rejected their help and gone to budgetary and administrative extremes to combat local assistance in enforcing immigration law.

More specifically, the Secure Communities, 287(g), and similar programs have been used only to the extent that they advance the enforcement priorities of this Administration. For example, Secure Communities requires the FBI to provide DHS with a copy of the fingerprint and criminal records of individuals who are picked up by local and state law enforcement officials for various crimes. DHS then runs the names of these individuals through its records to see if they are in the U.S. unlawfully or otherwise subject to deportation.⁴⁵

At this point, however, DHS begins to twist the law. If the individual is known to be in the U.S. illegally, ICE officers must go to the local jail and interview the individual in order to determine whether to pursue immigration charges. If an individual found through Secure Communities did not meet the Administration's enforcement priorities, he was simply allowed to remain in the United States. Essentially, all that local governments do is hold the individual for a few days and provide fingerprint information to the FBI as they normally would.⁴⁶ In April 2012, however, ICE announced that it would no longer ask local jails to detain unlawful immigrants who were stopped for "minor traffic offenses" and other lesser offenses, reducing Secure Communities' effectiveness.⁴⁷ Bizarrely, ICE also stated that

it would analyze and take steps against local jurisdictions where arrest-rate data was "abnormal," hinting at the idea that DHS would go after communities where the arrest rate of illegal aliens was too high, despite DHS's constant claims of limited resources.⁴⁸ Finally, in President Obama's executive actions in the fall of 2014, Secure Communities was formally discontinued, with ICE starting a new program that will have an even more limited scope. This program, called the Priority Enforcement Program (PEP), will cease to enforce any immigration offenses unless the individual is already a convicted criminal.⁴⁹

Even as the Secure Communities program has been removed as an immigration enforcement tool, the 287(g) program has been openly assaulted by the Obama Administration because it allows local and state officials to enforce U.S. immigration law. Local law enforcement officers must undertake training and enter into memorandums of agreement with ICE to receive immigration-law-enforcement authority; 287(g) officers are then authorized to arrest individuals and begin the removal process, essentially acting as an extension of ICE. This program is cost-effective at approximately \$68 million a year, and acts as a force multiplier for ICE.⁵⁰ But enforcing U.S. immigration laws against most illegal immigrants is exactly the opposite of DHS's stated immigration priorities. As a result, 287(g) has come under consistent attack from amnesty activists and the Obama Administration. President Obama's budget proposal has twice recommended steep cuts in 287(g), most notably for FY 2014 when the President's budget would have slashed \$44 million, almost two-thirds of the 287(g) program's budget.⁵¹

At the same time, the Obama Administration has sought to tie the hands of local governments by limiting how they enforce the law, or by simply ignoring or rescinding 287(g) agreements. In December 2011, DHS rescinded Arizona's Maricopa County's 287(g) agreement and restricted access to the Secure Communities program.⁵² Then, in June 2012, immediately following the Supreme Court's decision to uphold most of Arizona's immigration law, DHS rescinded all of its street-level 287(g) agreements in Arizona.⁵³ Since allowing local law enforcement officers to enforce the law is against DHS's Administration-mandated objectives, President Obama has used every tool to assault the 287(g) program to ensure that immigration laws are not enforced.

If the U.S. is to enforce its immigration law, states must be a part of the solution. Any Administration can and should expand 287(g) agreements and call on the assistance of state governments through other cooperative immigration-law-enforcement programs. Furthermore, rather than suing states for correctly enforcing the letter and intent of federal immigration laws, this and future Administrations should cooperate with and support state governments, and only take action against those states that are breaking immigration laws—such as by providing in-state tuition to illegal immigrants. At some point, Congress can follow up and expand cooperative programs by requiring DHS to accept requests from state and local governments to enter into a 287(g) agreement. Congress should also forbid DHS from providing grant money to cities that resist the enforcement of immigration law, known as sanctuary cities. While federalism gives local governments some latitude in choosing to oppose or not assist the federal government in enforcing immigration law, the federal government does not have to reward or pay for the results of such policies.

In addition to ERO, ICE's HSI office also conducts important work, though its missions are more in the vein of traditional law enforcement. In addition to various police, national security, and intelligence functions, ERO plays a unique role in the vetting of visa applications through the Visa Security Program (VSP) in HSI's international operations division. The VSP deploys HSI agents to critical embassies and consulates around the world to advise and assist State Department officials in the visa-adjudication process. HSI officers bring law enforcement and security expertise to high-risk diplomatic posts, and work with local law enforcement to further improve detection of potential threats stemming from that country. To this end, ICE had deployed about 250 special agents, as well 170 support staff to 62 offices throughout 26 countries in 2015. The VSP reviewed over two million visa applications, including 8,600 visa refusals, of which 2,200 were for suspected terrorist connections or activity.⁵⁴ The VSP program also participates in the Security Advisory Opinions (SAO) program, which provides additional scrutiny to high-risk applications. The PreAdjudicated Threat Recognition Intelligence Operations Team (PATRIOT) is a related program that brings together CBP, ICE, Intelligence Community, and State Department officials to investigate suspicious

visa applications. Making HSI resources and officers available to State Department visa officials should be expanded to improve vetting.

Actions for Congress. Ultimately, major changes in policy are required to fix ICE and the U.S. immigration system. ICE will also need greater funding to allow it to remove more illegal immigrants and ensure that those who remain in the country show up at their court hearings. Additional funding will also collapse the Obama Administration's claim that ICE is held back only by finite resources. Congress should:

- **Defund the President's executive actions on immigration enforcement.** The Obama Administration has issued a series of policy memorandums that do not allow ICE ERO officers to do their jobs. To improve morale and enforce existing immigration laws, Congress should prohibit any funding in support of these amnesty and non-enforcement policies. Failing to do so jeopardizes Congress's constitutional authority and sets a dangerous precedent that empowers the executive branch in ways that all Americans should fear.
- **Strengthen the 287(g) program.** Designed to make it easier for state and local governments to assist in enforcing federal immigration laws, 287(g) has been under assault during the Obama Administration, which has sought to cut funding, access to, and use of, the program. Congress should widen 287(g) usage by increasing funding for the program and requiring DHS to enter into a 287(g) agreement with any state and local government that requests entry, with significant consequences should DHS not meet this requirement in a timely fashion.
- **Increase rapid-removal authority.** Currently, Administration policy restricts ICE from removing many illegal immigrants in an expedited manner. To prevent future humanitarian and security crises on the border, ICE should be allowed to rapidly remove any illegal border crosser. This can be accomplished by making this authority explicit in section 235 of the Immigration and Nationality Act and by reforming the William Wilberforce Trafficking Victims Protection Reauthorization Act of 2008 to clarify that children who are not victims of human trafficking

should also be removed in an expedited manner to discourage future surges.

- **Provide more prosecutors and agents.** In addition to letting ICE agents do their jobs by removing non-enforcement policies, Congress should increase the number of ERO officers as well as a corresponding number of prosecutors and legal personnel to be able to expedite necessary removals. Additional agents for HSI will also allow the U.S. to expand the VSP to improve visa vetting.
- **Increase the number of illegal immigrants who appear at their court hearings.** While more detention beds guarantees that more individuals will show up to immigration proceedings, this system can be expensive. Increasing the use of the most effective ATD, such as GPS tracking anklets, in addition to detention facilities, is a cost-effective way of reducing the number of absconders.

To fund these activities, the Heritage budget recommends \$7 billion for ICE.

Additionally, Heritage recommends that Congress provide the Justice Department with additional funds for immigration court judges to support the work of increased ICE operations.

5. Transportation Security Administration

The President's FY 2017 budget requested \$7.59 billion for the TSA, slightly more than the FY 2016 appropriation of \$7.44 billion in total budget authority. Perhaps the DHS component most recognized by the general public, the TSA was created after 9/11 to protect U.S. transportation systems, including trains and buses, though aviation security is its prime focus.

The TSA could benefit from significant changes and reforms. Continuing to expand and strengthen trusted-traveler programs, such as PreCheck, will increase the time that TSA screeners spend on travelers of higher or unknown risk. The TSA should also be forced to expand the Screening Partnership Program (SPP) that saves the government money and enhances productivity by allowing airports to use private screeners (with TSA oversight) in place of TSA screeners. Additionally, Congress should rethink the 100 percent screening of air

cargo and provide more financial support to the Federal Flight Deck Officer (FFDO) program as a cost-effective supplement to the Federal Air Marshal Service (FAMS).

DHS has several trusted-traveler programs that give participating low-risk travelers access to streamlined security, customs, and immigration screening. These programs, including TSA PreCheck and CBP's Global Entry, NEXUS, and SENTRI, are all predicated on the concept of risk-based security. The U.S. could treat every individual who enters the U.S. as an equal potential threat to U.S. security, or it could differentiate between lower-risk individuals and those who present greater risks, or whose risk is simply unknown. This risk-based security allows the U.S. to use its limited security resources more efficiently.

TSA PreCheck generally ensures that participants receive an expedited screening process, including the ability to keep on shoes, belts, and light jackets, and to keep computers and liquids in their bags at roughly 160 participating airports and with 16 airlines.⁵⁵ To join PreCheck, individuals must apply in person at a TSA application center and undergo a background check, be enrolled in one of the other trusted traveler programs, or be a member of the military or a military academy. Additionally, PreCheck occasionally includes frequent travelers as well as unvetted individuals through a process known as "managed inclusion," which allows a number of random travelers to use the PreCheck line.⁵⁶ TSA PreCheck enrollment grew from around 4,000 travelers in December 2013 to 2 million in January 2016.⁵⁷ However, to make TSA PreCheck an efficient use of resources and effective at speeding up security lines, the TSA needs to further expand enrollment in the program.

While the TSA is continuing to expand PreCheck, concerns regarding security have been raised by the IG, the GAO, and independent researchers, especially after a serious criminal was able to pass through a PreCheck line after a faulty risk assessment declared him to be low risk.⁵⁸ As a result, the new TSA Administrator, Peter Neffenger, has ordered that managed inclusion be phased out with one part cancelled in late 2015.⁵⁹ Additional security assessments should be undertaken and heeded if PreCheck is to remain a beneficial tool to the TSA. Much of these assessments will have to be classified, but Members of Congress should be informed,

and unclassified findings should be made available when possible. Congress should address these classified findings regarding how it can mitigate risks in the PreCheck system.

The TSA also manages the screening of travelers and cargo. Unlike TSA PreCheck, a security policy that needs to be rethought is the 100 percent screening of air cargo. The TSA currently screens 100 percent of all domestic air cargo at levels “commensurate with screening of passenger checked baggage,” as required by the Implementing Recommendations of the 9/11 Commission Act.⁶⁰ The language of the act, however, was very broad and seemed to include international cargo, and the TSA is currently screening 100 percent of high-risk cargo, since complete screening at a hundred or more international airports would be extremely problematic from logistical and diplomatic perspectives. With the growth of capabilities, such as CBP’s Automated Targeting System, that determine the risk level of cargo by checking manifest and cargo data against a variety of intelligence databases, examining the nature of the cargo, its source, its destination, and other factors, the TSA should move from the costly and disruptive 100 percent scanning mandate to a risk-based approach. This approach would use risk factors and intelligence to determine which pieces of cargo deserve closer inspection, rather than treating all cargo as carrying the same risk.⁶¹ At the very least, the TSA should make it easier for companies to comply with the mandate, such as through the Certified Cargo Screening Program (CCSP), which would lessen costs and make cargo transportation easier and faster.⁶²

Famously, the TSA also scans passengers before boarding a flight—with poor results. John Roth, the DHS IG, stated in early 2015 that he was “deeply concerned” about the TSA’s inability to protect travelers, noting that the TSA has received over 100 warnings for its shortfalls.⁶³ He testified recently that:

We have conducted a series of covert penetration tests—essentially testing TSA’s ability to stop us from bringing simulated explosives and weapons through checkpoints, as well as testing whether we could enter secured areas through other means. Although the results of those tests are classified, we identified vulnerabilities caused by human and technology-based failures.

We have audited and reported on TSA’s acquisitions. Our audit results show that TSA faces significant challenges in contracting for goods and services. Despite spending billions on aviation security technology, our testing of certain systems has revealed no resulting improvement.

We have examined the performance of TSA’s workforce, which is largely a function of who is hired and how they are trained and managed. Our audits have repeatedly found that human error—often a simple failure to follow protocol—poses significant vulnerabilities.

We have looked at how TSA plans for, buys, deploys, and maintains its equipment and have found challenges at every step in the process. These weaknesses have a real and negative impact on transportation security as well.⁶⁴

The IG also found that the TSA’s efforts to vet airline workers have not been entirely successful. In a recent review of airline workers, 73 were found to be part of the larger Terrorist Identities Datamart Environment (TIDE), the government’s most comprehensive database on known and suspected terrorists. While these individuals were not part of the higher-risk Terrorist Screening Database, it is highly concerning that 73 airport employees may have links to terrorist activity.⁶⁵ The TSA has requested that it receive expanded access to additional parts of the TIDE.

Perhaps most worryingly, the TSA failed to stop weapons and bomb materials smuggled by undercover agents in 67 of 70 recent probes of airport security across the country. While Homeland Security Secretary Jeh Johnson announced that changes were being made,⁶⁶ and a new administrator has taken over, this dismal record calls into question the entire reason for the TSA’s existence. Such undercover “red team” exercises should be expanded and become a key metric for determining the success of airport security.

Such failures highlight the fact that the federal government and the TSA need not conduct front-line screening, as there is an effective and less costly alternative in the Screening Partnership Program (SPP) that substitutes private screeners with TSA oversight in place of TSA screeners. Created as a result of the Aviation and Transportation Security

Act of 2001, the SPP allows airports to opt out of federal screening so long as they can show that private screening will not cost more, compromise security, or harm the effectiveness of screening.⁶⁷

Despite its potential benefits and the TSA's current challenges, the SPP has had a rocky implementation, being suspended by the Obama Administration before Congress restored it.⁶⁸ As of January 2015, 21 airports were participating in the SPP.⁶⁹ There are multiple reasons why an increasing number of U.S. airports are using the SPP, including productivity, cost, and security. In terms of productivity, a case study by the House Transportation and Infrastructure Committee in 2011 found that SPP screening was as much as 65 percent more efficient than federal screening.⁷⁰ One reason for this productivity gap could be the higher level of attrition in the TSA than in private screening companies. A related factor in productivity could be better staffing measures, ranging from day-to-day scheduling to more efficient hiring and union practices. Beyond pure efficiency, SPP airports also report improved customer service.

Productivity also bleeds over into considerations of cost, since a more productive workforce with less attrition is less expensive to maintain and operate. Although TSA studies found SPP programs to be more costly than government screening, these studies were widely criticized, including by the GAO, for flawed methodologies. When some of these flaws were corrected, the TSA found SPP and government screening to be nearly equal in cost.⁷¹ Furthermore, the House Transportation and Infrastructure Committee study found that when considerations, such as increases in productivity were accounted for, the cost of the program fell dramatically. Together with smaller overhead costs and lower levels of attrition, the SPP is likely a financial boon for most airports.

Nearly every study undertaken, whether by the TSA or other organizations, has found that private screeners, while no silver bullet solution, are at least as good as, if not better than, government screeners at detecting security threats.⁷² It is also worth considering that, if a private contractor fails to provide adequate security, perhaps by failing a red team test, the contractor can be replaced. The same cannot be said of the TSA.

It is for all these reasons that the vast majority of European countries allow airports to provide their

own screening force or hire a contractor to provide it.⁷³ Unfortunately, the process for joining and renewing an SPP contract remains mired in bureaucracy, taking as long as four years.⁷⁴ In the U.S., rather than allowing an airport to determine the best way to provide screening, the SPP is micromanaged by the TSA, with the TSA selecting a screening contractor for each SPP airport. Furthermore, the TSA has given its workforce collective bargaining rights, pitting security and cost-effectiveness against labor demands.⁷⁵

Finally, the TSA is also responsible for last lines of defense in aviation security—the Federal Air Marshals and Federal Flight Deck Officers. While FAMs, highly trained agents who fly aboard some aircrafts, are relatively well known and provide an additional layer of security to some flights, FFDOs are much less well known. FFDOs are pilots or navigators who have been trained by the TSA to use firearms to stop a hijacking. FFDOs voluntarily join the program and must pay for a great deal of the costs of the FFDO program themselves, with estimates running as high as \$10,000.⁷⁶ The TSA is currently covering the cost of the training itself, as well as meals and lodging at federal law enforcement training centers, but not transportation or time off from work.⁷⁷ The result is that the cost of the FFDO program is estimated at a mere \$20 per flight, as opposed to the cost of a FAM of around \$3,000.⁷⁸ Expanding funding for the program could help train additional FFDOs and help cover some of the personal costs involved in becoming an FFDO.

Actions for Congress. To improve transportation security, Congress should:

- **Improve security assessments.** In order to ensure security and continue the growth of TSA PreCheck and risk-based security, the TSA must conduct proper security assessments and refine the screening and vetting process to minimize security risks. Red team and other covert exercises and testing should become a larger part of these assessments as such tests are an effective way to judge the success of airport security.
- **Embrace risk-based screening and security.** Efforts such as the Automated Targeting System, which would subject cargo to a risk rating that determines whether it should be given additional screening, are the way to improve air cargo

security. Congress and DHS should look for ways to move away from a blanket screening process. At a bare minimum, they should expand the Certified Cargo Security Program, which allows the private sector to more easily meet the 100 percent screening mandate. Congress and the TSA should also look to expand enrollment in TSA PreCheck to shorten airport security lines.

- **Simplify the SPP approval and contracting process.** The process for joining SPP should be streamlined to make it easier for airports to apply, and to make TSA adjudication and processing faster, fairer, and more consistent. Airports joining the SPP should also be allowed to select and manage their own screening contractors from a list of TSA-approved companies, instead of continuing the TSA's micromanagement of the program.
- **Limit collective bargaining.** Collective bargaining in the screening line is harming security and costing taxpayers and travelers. Congress should expressly forbid the TSA from bargaining collectively.
- **Expand the FFDO program.** Greater funding for FFDO will enable this extremely cost-effective program to expand significantly.
- **Review alignment of the TSA budget with the risks.** TSA resources for any given activity should match the relative level of risk that that activity is working to mitigate. This requires the TSA, its IG, or the GAO to examine classified risk assessments and realign funding to better match the severity of different risks.

To fund these activities, the Heritage budget recommends \$7.5 billion for the TSA.

6. Coast Guard

With a budget of approximately \$11.1 billion in FY 2016 (President Obama requested \$10.3 billion for FY 2017), the Coast Guard is a unique part of DHS: It is the only military branch that is not a part of the Department of Defense. It has a variety of missions, including interdiction of narcotics and other illicit trafficking, search and rescue, maintaining safety and security in the Arctic, and providing

port security. With such a wide range of missions, the need for meeting Coast Guard modernization goals is great. Unstable and underfunded budgets have strained the Coast Guard's operational availability in recent years. This is particularly the case with a few major vessel programs, such as the Offshore Patrol Cutter (OPC) and the Fast Response Cutter (FRC). Congress should ensure that the Coast Guard has the resources it needs to protect U.S. waters and provide for the common defense. Without funding the Acquisition, Construction, and Improvements (AC&I) budget at the minimum level that the Coast Guard says is necessary—\$1.5 billion—it will continue to fall behind in recapitalizing the fleet.

Critical Platform Funding Reforms. Critical platform funding reforms are needed for the OPC, the FRC, unmanned aerial systems (UASs), and polar icebreakers.

Offshore Patrol Cutter. According to Coast Guard Commandant Admiral Paul F. Zukunft, the OPC is the Coast Guard's "number one acquisition priority."⁷⁹ The Coast Guard's program of record (POR) states that 25 OPCs are necessary to replace the service's 29 medium-endurance cutters (WMECs).⁸⁰ However, continued irregularities and delays in the program's funding cycle have pushed back initial procurement from 2016 to 2018—meaning that they will not be operational until at least 2021.⁸¹ It is therefore crucial that the Coast Guard strive to begin replacing the legacy craft in this cutter class, some of which are more than 50 years old. Furthermore, alternative analyses of the Coast Guard's capacity suggested that between 32 and 57 OPCs are necessary to meet mission while accepting different levels of risk.⁸² This year's budget proposal takes a step in the right direction for OPC, requesting \$100 million to begin purchasing long-lead-time material, and continued review of progress and design details. Congress should ensure that this is sufficient to begin procuring OPCs by FY 2018.

Fast Response Cutter. Though the Fast Response Cutter is being produced at a high rate, the Obama Administration continues to underfund this program in order to pay for other priorities. As Coast Guard officials have mentioned in the past, the FRC program should continue to procure six vessels per year to both replace legacy craft and to yield better economies of scale.⁸³ In FY 2017, the Coast Guard requested funding only for four—\$240 million

instead of the \$325 million that had been previously proposed. This is interesting because the value of two FRCs (roughly \$108 million) is near the amount requested this fiscal year for the polar icebreaker program (\$150 million), indicating that there is an unofficial ceiling imposed on the Coast Guard AC&I budget despite commandants consistently calling for an increase to it. Because the icebreaker has become a larger priority by nature of President Obama's order to accelerate its production, the FRC request was possibly cut to make this happen. The Coast Guard should not have to make short-sighted sacrifices elsewhere in its AC&I budget to pay for the icebreaker.

Unmanned Aerial Systems. The Coast Guard would also benefit greatly from procuring UASs to support NSC operations. According to the GAO, "Coast Guard officials acknowledged that the lack of [cutter-based] unmanned aircraft would create a gap between the NSC's actual and planned capabilities."⁸⁴ Dr. William Posage, program manager for the Coast Guard Research and Development Center, explained that the lack of cutter-based UAS technologies "left the NSC with an enormous surveillance gap in her ability to perform her mission."⁸⁵ Notably, the operational effectiveness of the NSC without a UAS component would "be comparable to that of the 378-foot Hamilton class high-endurance cutter," the very program it was designed to replace with capability enhancements.⁸⁶

The Coast Guard has successfully tested the FireScout and ScanEagle UAS platforms, both of which would significantly amplify the NSC's surveillance, detection, classification, and prosecution capabilities. Widely used for similar naval operations, they have successfully contributed to a handful of at-sea Coast Guard demonstrations. According to an assessment by the Coast Guard Office of Aviation Forces, the presence of two vertical take-off FireScout UASs aboard an NSC would enable the cutter to cover three times the presence radius of an NSC without them.⁸⁷ Similarly, according to a Senate Appropriations Committee report, "[t]he Coast Guard has reported...that its long standing plan to add vertical take-off unmanned aircraft systems to the National Security Cutters would result in an estimated 95- to 225-percent increase in surveillance coverage within an 800 nautical mile radius of the cutter and an estimated 95-percent increase in the number of prosecutions achieved by the cutter."⁸⁸

The Coast Guard's FY 2017 budget justification states that funding for the NSC program will in part "establish sUAS [small UAS] capability aboard one NSC, to include engineering analysis, non-recurring engineering, procurement and installation of sUAS components, and system testing and certification."⁸⁹ Admiral Zukunft testified before the House Transportation Committee in March 2016 that this activity would involve a "down select" for a sUAS capability "that will go on board" the NSC.⁹⁰ The NSC will amplify its aerial ISR capabilities dramatically with the longer-term integration of sUAS, while the sea service should continue to evaluate the vertical unmanned aerial vehicle (VUAV) platform.

Polar Icebreakers. The Coast Guard requires at least three heavy and three medium polar icebreakers to fulfill its polar missions.⁹¹ Currently, it only operates one of each.⁹² Given increasing economic, safety, and security interests in the Arctic, the need for icebreaking capacity will only increase in the future. President Obama announced during his trip to Alaska in 2015 that he is directing the government to accelerate procurement of one heavy polar icebreaker from FY 2022 to FY 2020.⁹³ Rough estimates have found that one heavy polar icebreaker built in the U.S. would cost around \$1 billion.⁹⁴

This year, the Coast Guard requested \$150 million for the heavy polar icebreaker, much higher than amounts in previous years, partly driven by the President's direction to accelerate it. While this displays a more legitimate commitment to fielding this capability, the government should make sure that it looks at all options to build it. This should include foreign shipbuilding companies, some of which have had consistent experience building such vessels and therefore purportedly can construct icebreakers at much lower cost than can the U.S.⁹⁵

As mentioned, there appears to be a ceiling for overall acquisition funding imposed upon the Coast Guard, possibly by DHS or the Office of Management and Budget. The Coast Guard has repeatedly stated that a minimum of \$1.5 billion (and upwards of \$2.5 billion) for AC&I is necessary to continue to recapitalize the fleet at an acceptable rate.

The program of record itself accepts a significant amount of risk with which Congress may not be comfortable. If Congress does not want to accept that much risk, it will need to revisit the alternative fleet mix analyses, that is, fleet sizes larger than the current program of record that the Coast Guard has

studied. Congress will then need to work with the Coast Guard to determine how additional funding for ships and platforms can best reduce risk, and provide the necessary funding level accordingly. Since the Heritage DHS budget is finding significant savings elsewhere, there is room for more funding should the Coast Guard and Congress believe that it requires a fleet size beyond that of the current program of record.

Actions for Congress. To improve USCG effectiveness, Congress should:

Recapitalize the Coast Guard. Funding for acquiring new Coast Guard vessels has been regularly short of what is necessary to complete the Coast Guard's mission, and often results in additional acquisitions inefficiencies and costs. Congress should commit to providing the Coast Guard with consistent acquisitions funding so that the USCG will have the vessels it needs to complete its missions. Congress should also ensure that any additional resources it provides to the Coast Guard are used to meet important priorities, including cost-efficient acquisition of the FRC, OPC, and unmanned systems.

To fund these activities, the Heritage budget recommends \$10.85 billion for the USCG:

- **A minimum of \$1.5 billion for AC&I.** This funding should include six FRCs, a clearer path to fielding OPCs more rapidly, a cost-effective icebreaker program for meeting icebreaking requirements, and robust investments in aviation assets, particularly unmanned systems.
- **\$7.06 billion for operating expenses.** FY 2016 appropriations included \$7.06 billion for operating expenses, including \$160 million for Overseas Contingency Operations. The Heritage budget maintains this level of OCO funding for 2017.
- **The USCG should maintain funding for other programs.** Environmental compliance, reserve training, health care, retirement pay, and other programs are funded at levels requested by the President.

7. U.S. Secret Service

The U.S. Secret Service's total funding fell slightly in the President's FY 2017 budget (to \$2.16 billion) from FY 2016's level of almost \$2.2 billion. The USSS is well known for its protective mission, but it is also responsible for combatting currency counterfeiting

and other financial crimes. Its protective mission currently faces numerous challenges, springing from multiple high-profile security failures in the past several years. While the Secret Service has had three different directors over the past three years, embarrassing incidents continue. Despite a review commission in the fall of 2014 and ongoing bipartisan scrutiny in Congress, the Secret Service seems to continue to slip, requiring more substantial changes and reforms to restore the Secret Service to the level of excellence for which it has typically been known.

A short chronology of the Secret Service's recent failures includes:

- **November 2009.** Husband and wife Tareq and Michaela Salahi attended a state dinner at the White House and met with President Obama—despite the fact that they were not on the guest list.⁹⁶
- **November 2011.** A man with a semi-automatic rifle fired at the White House, with at least seven bullets hitting the building. While Secret Service agents initially rushed to respond with weapons drawn, they were told to stand down by their supervisors—who attributed the shooting sounds to backfiring vehicles. Some agents dispute this account while others remain silent “for fear of being criticized.”⁹⁷ At the time, the President's daughter Sasha was at home, and his other daughter Malia was expected home soon. Despite the fact that the shooter's vehicle and gun were found within 10 minutes, an investigation was not initiated until a housekeeper noticed broken glass and bullet holes four days later.⁹⁸
- **April 2012.** Secret Service agents who were a part of President Obama's advance team to Cartagena, Colombia, engaged in sexual conduct with prostitutes.⁹⁹
- **May 2013.** A Secret Service supervisor removed ammunition from his gun and left a bullet in a woman's room at the Hay-Adams Hotel across the street from the White House and allegedly tried to force his way back into the room to retrieve it. Further investigation reveals that this same supervisor and another Secret Service official sent sexual e-mails to a female subordinate, resulting in their suspension.¹⁰⁰

- **March 2014.** Three Secret Service agents in Amsterdam were disciplined after a night of heavy drinking that left one agent passed out in a hotel hallway just one day before President Obama arrived.¹⁰¹
- **September 2014.** The Secret Service was unaware that an armed security contractor with a criminal record was on the same elevator as President Obama during a trip to Atlanta.¹⁰² Several days later, a fence jumper managed to run into the inner rooms of the White House before being taken down by an off-duty agent. Reportedly, the alarm system was turned off because it bothered White House staffers.¹⁰³
- **October 2014.** New information surfaced about the 2012 prostitution scandal involving Secret Service agents in Colombia indicating that White House aides knew about the involvement with prostitutes but did not investigate, and possibly interfered with other investigations.¹⁰⁴
- **March 2015.** Two senior Secret Service agents drove a government vehicle into the barricades outside the White House on March 4. The agents, including Marc Connolly who was the second-most senior agent on President Obama's security detail, appeared to be drunk and according to news reports, had just come from a party where alcohol was consumed.¹⁰⁵ Rather than arrest the officers and conduct sobriety tests, however, the supervisor on duty ordered that the agents—Connolly and George Ogilvie—be sent home. An investigation into the incident has concluded that “it was more likely than not that Connolly and Ogilvie’s judgment was impaired by alcohol,”¹⁰⁶ resulting in Connolly’s resignation.¹⁰⁷ Then on March 31, a manager in the Secret Services security clearance division was accused of sexually assaulting a female employee after returning to the office with her after a party. The manager is currently being investigated by the IG and Washington, DC’s sex crimes unit.¹⁰⁸
- **April 2015.** A Secret Service officer was charged with first-degree attempted burglary and destruction of property stemming from a domestic dispute with the officer’s ex-girlfriend.¹⁰⁹ In a separate incident, following a congressional hearing on Secret Service failures led by Chairman Jason Chaffetz, Chaffetz’s application to the Secret Service was

accessed about 60 times in March and April 2015 in contravention of privacy laws, and information in it was shared with others, including at least one person outside the Secret Service.¹¹⁰

With this record of embarrassing security incidents and the underlying problems that are creating them, morale at the Secret Service has plummeted, possibly to an all-time low. In the Partnership for Public Service’s 2011 survey of the Best Places to Work in the Federal Government, the Secret Service was considered an above-average place to work. Steadily declining since then, in the 2015 survey, it plummeted to 2nd-worst agency for which to work in the federal government.¹¹¹

As these incidents began to pile up, Homeland Security Secretary Johnson ordered a review of the Secret Service. A review panel found three major problem areas:

1. Training and personnel;
2. Technology, perimeter security, and operations; and
3. Leadership.¹¹²

The panel found that the amount of on-the-job training for both the Presidential Protective Detail (PPD), and the Uniform Division that protects the White House and other sites, have “fallen below acceptable levels.”¹¹³ The panel also found that there were too few agents and officers to both meet mission needs and have time for training. The review panel and the Secret Service are unable, however, to appropriately size its force since the relevant data are not available. The review panel recommended increasing the number of agents and officers by about 285, but noted that this would be just the first step toward right-sizing the service. The panel also found that the White House fence was not tall enough nor designed appropriately to hinder or stop potential intruders, a problem at least partially addressed by the addition of spikes to the fence in the summer of 2015.¹¹⁴

But the most important finding of the panel was that “[f]rom agents to officers to supervisors, we heard a common desire: More resources would help, but what we really need is leadership.” The review panel believed that leadership and accountability by the director of the Secret Service to every agent is the

priority. To this end, the panel recommended that the next Secret Service director come from outside the service, to ensure that an “honest top-to-bottom reassessment” of the service could be completed.¹¹⁵ The review panel found that increased interaction with relevant experts outside the Secret Service and improved administrative capabilities would help to improve efficiency and effectiveness. Particularly, accountability must be re-instilled in the management ethos of the service since “accountability creates the culture of performance that the Secret Service needs to meet its zero-failure mission.”¹¹⁶

Despite the recommendation for a director from outside the service, President Obama chose the former head of the PPD, Joseph Clancy, as the new director. This does not mean that the Secret Service cannot be fixed under Director Clancy, who certainly has the experience and expertise to do so, but that the level of true soul-searching and complete reassessment of the agency may be more difficult. That said, it is too early to know if Director Clancy is taking the right steps.

Actions for Congress. To support the reform of the U.S. Secret Service, Congress should:

- **Increase Secret Service staffing.** The review panel recommended 85 more PPD agents and 200 more officers, but called on the service to create a mission-based budget that will determine the appropriate staffing levels.
- **Mandate increased training.** The panel called for PPD agents to spend 25 percent of their on-duty time in training, the so-called Fourth Shift. For the officers, a minimum of 10 percent on-duty training time should be required.
- **Require increased disciplinary and accountability standards.** When improper behavior or mistakes are made, the Secret Service should demand a strict disciplinary or corrective action. Supervisors and managers must be made to uphold these standards or be held accountable themselves. Congress should require the GAO to report on how these standards are employed and whether they are instilling discipline across the service.
- **Expand the number of professional administrators, rather than agents or officers, responsible for budgeting and workforce functions.** The review panel points out that

agents and officers may not always be the best at completing administrative tasks, and that a larger suite of professional administrators could support and improve planning and execution of core responsibilities.

- **Provide continued oversight to ensure that reforms are completed thoroughly.**

To fund these activities, the Heritage budget recommends \$2.2 billion for the USSS.

8. National Protection and Program Directorate

The National Protection and Program Directorate (NPPD) received approximately \$3.08 billion in FY 2016, and President Obama’s FY 2017 request calls for a slight decrease, to \$3.04 billion, though this decrease is largely explained by a request to transfer the Office of Biometric Identity Management from the NPPD to CBP. The NPPD is the primary component of DHS that is responsible for cybersecurity and the protection of critical and government infrastructure. While the NPPD has this responsibility, the vast majority of critical infrastructure (generally estimated at more than 90 percent) is owned and operated by the private sector.¹¹⁷ As a result, the NPPD, whether it is working in cyberspace or securing a chemical facility, often supports, collaborates with, or regulates private-sector efforts. The NPPD also protects federal facilities, both in cyberspace and physical locations, and manages DHS’s primary biometrics database, IDENT.

Cybersecurity. The NPPD is the primary hub for cybersecurity, not only for DHS, but for all civilian government agencies. Within the NPPD, the Office of Cybersecurity and Communications (CS&C) is the primary office managing cyber operations, with support from the Office of Cyber and Infrastructure Analysis. CS&C is tasked with leading the effort “to protect the federal ‘.gov’ domain of civilian government networks,” and also works with the private sector to protect critical infrastructure and businesses. Much work remains to be done in this area, both in DHS and across the federal government, as a recent study found that government cybersecurity rated worst in a study of 18 major industries.¹¹⁸

Within CS&C, the primary hub of cybersecurity operations is the National Cybersecurity and Communications Integration Center (NCCIC). The NCCIC is

“a 24x7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the Federal Government, intelligence community, and law enforcement.”¹¹⁹ The National Cybersecurity Protection Act of 2014 formally made the NCCIC a hub for sharing and receiving information from the private and public sectors, improving awareness and preparedness for cyber vulnerabilities, threats, and mitigation options. With the passage of the Cybersecurity Information Sharing Act (CISA), which provides additional protections for those that share information, and additional procedures for that sharing and spread of information, the NCCIC will assume an even more central role in sharing cyber information with others in government and the private sector.¹²⁰ In addition to sharing information on cyber threats and vulnerabilities, the NCCIC also contains the United States Computer Emergency Readiness Team (US-CERT) and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). As their names imply, these organizations specialize in responding to major cyber incidents in order to stop or mitigate a breach or an attack; both CERTS also work to prevent cyber incidents by sharing cybersecurity information with public-sector and private-sector partners.

CS&C also has two offices—(1) Federal Network Resilience and (2) Network Security Deployment—focused on defending federal networks, as DHS was charged in 2010 with overseeing the cybersecurity of federal civilian agencies. To this end, CS&C runs multiple programs including the National Cybersecurity Protection System, more commonly known as the Einstein family of systems. Einstein 1 focused on passively collecting information on network traffic of government organizations. Einstein use corresponded with the implementation of the Trusted Internet Connection (TIC) initiative in the mid- and late 2000s, which sought to have data flowing into government networks through 50 separate Internet gateways, a measure that makes it easier for the government to monitor data flowing to and from government computer networks and stop malicious behavior.¹²¹ Einstein 2 built on these capabilities by detecting intrusions and malicious computer network activity that came through the TICs. Einstein 3 Accelerated (E3A) is now being implemented; it is intended to prevent and disrupt intrusions into federal networks by using threat and vulnerability signatures to find malicious behavior.¹²²

A recent GAO report, however, indicated that Einstein faces multiple difficulties. The GAO found that Einstein was unable to detect a worryingly large number of potential threats and vulnerabilities. For example, for five applications (Adobe Acrobat, Flash, Internet Explorer, Java, and Microsoft office), only 6 percent of known vulnerabilities were covered by Einstein.¹²³ The GAO found that Einstein was not drawing on important sources of vulnerability information, such as the National Vulnerability Database (NVD) held by the National Institute of Standards and Technology (NIST) or DHS’s Continuous Diagnostics and Mitigation (CDM) program that detects vulnerabilities in federal systems, such as poor passwords or unpatched systems.¹²⁴ DHS said that it is working to incorporate additional sources into its databases, and noted that Einstein should not be the only security system a department uses.

Beyond difficulties with vulnerability and threat signatures, the GAO also found that Einstein was enabled at only five of the 23 customer departments, and even among those five some types of Web communications, such as e-mail, were not being monitored. Much of this difficulty lies in the dual responsibility for cybersecurity that lies with DHS and each department. While DHS’s cyber programs can provide some level of security for .gov domains, each department is responsible for much of its own cyber activity, including how well it uses programs like Einstein. The GAO recommended that DHS provide better guidance to other departments on how to ensure that online traffic is routed through Einstein sensors.

Additionally, Einstein is only a signature-based system that does not use anomaly-based or stateful-purpose detection methodologies, which are more complex approaches that “involve comparing current network activity to predefined baselines of ‘normal behavior’ to identify deviations that could be indicative of malicious activity.” These approaches to intrusion detection are more effective than signature-based detection in identifying previously unknown threats, such as “zero-days” or attacks that have no patch or fix.¹²⁵ DHS stated that it is piloting new technologies to detect anomalous network activity and build upon Einstein.

CS&C also runs the Enhanced Cybersecurity Services (ECS) program in order to improve the cybersecurity of owners and operators of critical infrastructure.¹²⁶ ECS does so by providing classified and

sensitive cyber threat information to approved commercial service providers—currently AT&T, Verizon, and CenturyLink—that can provide better security services to critical infrastructure.

For quicker automated sharing of threat data among and between the private and public sectors, CS&C is working with the MITRE Corporation on the STIX and TAXII systems. STIX is essentially a common language that can be used to detail threats,¹²⁷ while TAXII enables automatic sharing of data in the STIX format.¹²⁸ The goal of STIX and TAXII is to make information sharing as quick and helpful as possible, with the added privacy advantage of minimizing personal information and focusing sharing on the coding of threats and threat actors.

DHS is also responsible for the Critical Infrastructure Cyber Community (C3) Voluntary Program, which promotes the adoption of the National Institute of Standards and Technology's (NIST) Cybersecurity Framework.¹²⁹ Created by Executive Order 13636, the framework designed by NIST and supported by DHS is primarily built around a voluntary set of cybersecurity standards and best practices.¹³⁰ These standards were created by NIST; DHS's role is to encourage their adoption generally, while sector-specific agencies, such as the Department of Energy, may use existing regulatory authority to apply the standards to the energy sector.¹³¹

Though the NPPD operates these and other cybersecurity programs, it has not done so without challenges. As with many other DHS organizations, the NPPD as a whole must deal with the crippling problem of poor workplace satisfaction. In the 2015 Best Places to Work in the Federal Government, the NPPD rated 312 of 320 subcomponents. While relatively low pay at higher levels may be an issue, especially in the cyber field, the NPPD employees complained mainly about the lack of leadership, training, and performance-based rewards. Indeed, in October 2013, the DHS IG also found that, due to a lack of funding, the training of employees at the NCCIC was not providing NCCIC personnel with the specialized training they needed.¹³² Together with bureaucratic hiring processes, the NPPD has trouble finding and keeping trained and talented cybersecurity professionals, especially at more senior levels.¹³³ Congress tried to ease this problem by passing a cyber workforce measure that made pay more competitive for cyber positions, and called for a strategy to identify, hire, and keep skilled experts.¹³⁴ Communication

with the NCCIC seems to indicate that DHS has made progress in the past few years in building a team of qualified professionals, but the workplace dissatisfaction will continue to limit the effectiveness of operations.

Additionally, there are concerns about the effectiveness and speed of CS&C's operations. For example, in the past, US-CERT has been widely criticized for only sharing information provided by the private sector after considerable delays, though this criticism has decreased recently.¹³⁵ The GAO found in 2014 that, though federal entities are generally satisfied with US-CERT's responses to incidents, it is hard to determine just how effective US-CERT is due to a lack of evaluation measures.¹³⁶ Additionally, while Einstein is continuing to spread across federal systems, unnecessary delays and bureaucratic barriers still exist. This was made evident during the 2014 Heartbleed vulnerability incident. While Einstein was able to detect the Heartbleed computer bug, Phyllis Schneck, the Deputy Under Secretary for Cybersecurity and Communications for the NPPD, stated that it took almost a week until some other government agencies let the NCCIC and Einstein search for problems.¹³⁷ Other concerns include the slow adoption of the ECS program, though the IG found that DHS is making headway on improving the program and is meeting the IG's recommendations.¹³⁸

The GAO has issued multiple reports noting significant flaws in cybersecurity measures and in incident response and mitigation procedures.¹³⁹ Similar to the example of Einstein and Heartbleed, DHS needs to have greater authority and more robust relationships with government organizations so that DHS can help those agencies secure their systems and respond to security incidents. The recent discovery of a major breach of the Office of Personnel Management (OPM) database, however, has raised questions about the efficacy of the Einstein program. It appears that OPM did not have access to the latest generation of Einstein, but experts still wonder why the existing program was unable to detect so much information being exfiltrated from government servers.¹⁴⁰ While Einstein is still an important tool in the cybersecurity arsenal, this major data breach should reinforce the idea that there is no silver bullet to cybersecurity.

CS&C also manages communications networks and emergency communication systems. The

National Coordination Center for Communications maintains communications systems during natural disasters and after terror or cyber attacks.¹⁴¹ The Office of Emergency Communications (OEC) on the other hand, works primarily with emergency responders throughout all levels of government to ensure that interoperable communications are available in the event of an emergency.¹⁴² However, the IG reported in 2012 that only one of 479 DHS radio users could find and use a common channel to communicate with each other. When the radios were analyzed, 54 percent did not have the DHS Common Channel programmed into the radio, and 26 percent had other problematic settings. Similarly, 29 percent did not have the Federal Interoperability Channel programmed, and 45 percent had other flawed program settings for communicating over that channel.¹⁴³

While some improvements have been made, the IG reviewed DHS's progress and in May 2015 found that the IG's recommendations were only partly implemented and that most DHS radio users could still not access the DHS common radio channel.¹⁴⁴ The IG recommended to the Under Secretary of Management that more authority be given to the OEC and other coordinating bodies to "ensure that components achieve interoperability," though DHS disagreed with this recommendation. This recommendation is similar to Heritage's recommendation for DHS management that centralized service offices receive more authority to ensure that all components are implementing department-level policy. With a stronger coordinating structure, the IG also recommended improving policies governing the standardization of DHS radio activities and settings.

Infrastructure Protection. The NPPD's Office of Infrastructure Protection (IP) is the lead organization in the U.S. government for the protection of critical infrastructure.¹⁴⁵ The U.S. has 16 critical infrastructure sectors:¹⁴⁶

- **Chemical**
- **Commercial Facilities**
- Communications
- **Critical Manufacturing**
- **Dams**

- Defense Industrial Base
- **Emergency Services**
- Energy
- Financial Services
- Food and Agriculture
- Government Facilities
- Health Care and Public Health
- Information Technology
- **Nuclear Reactors, Materials, and Waste**
- Transportation Systems
- Water and Wastewater Systems

DHS is responsible for 10 sectors; the IP is responsible for six (indicated in bold). The NPPD also coordinates critical infrastructure policies across all sectors, following the guidance of the National Infrastructure Protection Plan (NIPP) and PPD-21.¹⁴⁷

To protect critical infrastructure, sector-specific agencies should:

- "Facilitate the public-private partnership across critical infrastructure sectors;
- "Develop strategic goals to mitigate risk and improve resilience;
- "Provide and promote education, training, information sharing, and outreach support;
- "Shape sector-specific goals that address physical, human, and cybersecurity risks and drive security and resilience activities and programs;
- "Provide, support, and facilitate technical assistance and consultations to identify vulnerabilities and mitigate incidents;
- "Implement the NIPP 2013 framework and guidance tailored to respective sectors;

- “Develop sector-specific plans with public and private sector partners.”¹⁴⁸

While these sector-specific agency activities are primarily voluntary, agencies may also have additional regulatory authority to mandate certain activities. Within IP, the Infrastructure Security Compliance Division (ISCD) is one example of such authority, as it enforces the Chemical Facility Anti-Terrorism Standards (CFATS) governing the chemical sector.

CFATS is supposed to operate by ranking chemical facilities according to their level of risk, that is, the threats they face, the vulnerabilities in their security systems, and consequences of an attack on the facility. Once facilities are grouped into four risk tiers, each facility is required to improve its security by meeting 18 performance standards through a site-security plan or an alternative security program (ASP). While in theory this risk-based type of regulation is preferable to one-size-fits-all mandates, CFATS has fallen far short.

In April 2013, the GAO reported significant problems with the risk-based system that underpins CFATS. Specifically, the GAO found that in considering and analyzing risks, DHS did not consider economic consequences, failed to identify or include vulnerabilities, and assessed threats inconsistently. In other words, the risk assessment that is central to CFATS failed on all three elements of risk: threat, vulnerability, and consequences.¹⁴⁹ The GAO report also found that DHS outreach to chemical facilities was generally not useful.¹⁵⁰ The same report calculated that even if the ISCD dramatically increased its reviews of security plans, it would take between six-and-a-half years and nearly nine years to completely approve the plans, not to mention conducting compliance inspections and making changes in risk tiers.¹⁵¹ In addition to these problems, the ASP program, which industry thought would be more widely used, has been restricted, forcing more low-risk facilities to undertake additional security precautions regardless of whether existing security upgrades could have been effective alternatives.¹⁵² Finally, of the 18 CFATS standards, the ISCD struggled to create and implement the Personnel Surety Program, confusing chemical facilities and delaying the approval of security plans.¹⁵³

In 2014, Congress tried to resolve some of these issues. The Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014 attempts to

clarify and expand the use of ASPs, and simplifies the personnel-surety standard¹⁵⁴ by allowing a chemical facility to use other government screening programs as a way to meet CFATS requirements.¹⁵⁵ In addition, the act attempts to speed up the approval process with expedited approval for lower-risk tiers. DHS has also taken action to shorten the backlog, though GAO has yet to report on the effectiveness of these changes.¹⁵⁶ While the act calls for a proper risk assessment, it is unclear whether DHS will be successful this time around.

Federal Protective Service. The NPPD is also responsible for protecting over 9,500 federal facilities across the U.S. With around 1,000 full-time law enforcement positions and 13,000 contractors, the Federal Protective Service (FPS) is a significant part of the federal security force, but it can also delegate security responsibilities and allow agencies and facilities to manage security themselves. The FPS is currently funded by fees it collects from the agencies and facilities it protects.¹⁵⁷

Beyond the cybersecurity risks identified by the GAO (mentioned above), the FPS has significant challenges. According to *Roll Call*, between 2010 and 2012, the “GAO made 26 recommendations relating to FPS risk assessment programs and oversight of guards’ training, certifications and qualifications.”¹⁵⁸ As of April 2016, the GAO has at least 23 open recommendations for the FPS, with eight ranging back to 2012.¹⁵⁹ As mentioned, these areas in need of improvement center on how well the FPS assesses risk, budgets and plans, and manages and oversees its security forces and activities central to its protective mission. For example, the GAO found in September 2013 that five of 16 guard companies had not received active shooter training, while other companies’ guards had not been trained in the use of screening equipment.¹⁶⁰ The GAO reviewed a sample of guard files, also in 2013, and found that 23 percent were missing some “required training or certification documentation.”¹⁶¹ Multiple recommendations concerning these issues remain unresolved. More recently, in a March 2015 report, the GAO found that the FPS was not managing its delegations of security responsibility effectively. The GAO reported that the FPS claimed that 62 delegations of security responsibility were active, but included 12 delegations that had expired or been rescinded.¹⁶²

In what could be viewed as a significant vote of “no confidence,” a May 2014 DHS memo announced that the FPS would no longer be directly responsible

for security at DHS headquarters.¹⁶³ While this was disputed by the FPS, such news is merely one of many concerns that the FPS must navigate if it is to improve its operations.

Biometric Identity Management. The NPPD's Office of Biometric Identity Management (OBIM), called US-VISIT until 2013, is responsible for managing the U.S.'s biometric data system, the Automated Biometric Information System (IDENT). IDENT is used to collect biometric data from individuals as they enter the U.S. for a variety of immigration purposes as well as for counterterrorism and security purposes.¹⁶⁴ To these ends, IDENT is closely integrated with the FBI's Integrated Automated Fingerprint Identification System (IAFIS).¹⁶⁵ IDENT, however, was created in 1994, and though it has made remarkable improvements over the years, DHS's Chief Information Officer has seen continuation of this aging system as a growing risk due to increasing demands and technical limitations.¹⁶⁶ With that in mind, the NPPD is looking to begin replacing IDENT, which should lower maintenance costs and improve capabilities.¹⁶⁷ President Obama recommended that OBIM be shifted to CBP in his final budget request, as NPPD is not the best fit for the office.

Before moving this office, DHS should consider a larger-scale streamlining and upgrading of its vetting and immigration casework systems. With systems from CBP's TECS, USCIS's ELIS and asylum claims systems, NPPD's IDENT, and other systems facing challenges or the need for updates, DHS should develop a more cohesive and integrated set of systems. One way this could be done is to embrace a person-centric model that allows DHS organizations, when investigating or vetting an individual, to query the person rather than various systems. A person-centric system would pull information from each DHS component so the investigator or adjudicator has all the necessary information in one place. The TSA is working on adopting this approach in its intelligence and screening efforts,¹⁶⁸ and other parts of DHS have considered such a system as well.¹⁶⁹ DHS would be wise to expand such efforts over the entirety of DHS and determine the resources that will be needed to implement such a system.

Actions for Congress. To improve the U.S.'s cybersecurity and security of critical infrastructure, Congress should:

- **Implement cyber-threat and cyber-vulnerability information sharing.** CISA allows the private

sector and public sector to more easily share information with each other, benefitting both sides. By providing strong liability protection for shared information, businesses will be encouraged to share with the government as well as with other businesses.

- **Help DHS improve and expand its ability to monitor government networks.** The DHS-run Einstein intrusion-detection-and-prevention system has grown dramatically over the past decade. With better information sharing, Einstein's ability to detect and prevent intrusions would be enhanced, but the system must connect to other sources, such as NIST's NVD and DHS's CDM. Additionally, Congress should encourage DHS to expand the traffic that Einstein monitors and the types of methodologies it uses to detect malicious activity. Congress should prioritize the continued improvement and expansion of the Einstein system. DHS needs the clear authority, relationships, and ability to work with other agencies in using Einstein and other cyber tools.
- **Improve morale of DHS staffers.** Morale at the NPPD is incredibly low, which makes it difficult to recruit and keep good employees, especially when private-sector cybersecurity jobs are available. Notably, pay is not the central issue in this survey. The lack of leadership, training, and performance-based rewards are blamed, and to the extent that Congress can do so through the budget process, it should mitigate these problems. For example, Congress should ensure that funding for performance-based rewards and training is sufficient. If DHS is to be an effective actor in defending U.S. cyberspace and critical infrastructure, more must be done to improve morale and maintain a highly skilled workforce.
- **Reform risk assessments to capture all relevant information, including consequences, threats, and vulnerabilities.** DHS has a history of conducting risk assessments poorly, and this systemic problem must be resolved. Not correcting this problem will mean that important security decisions are made with inaccurate and incomplete information. Trouble with risk assessments at the FPS and ISCD severely hamper the efforts of the NPPD to protect critical infrastructure.

- **Improve interoperable communications policies.** The OEC and coordinating bodies must have more authority to insert policy into each DHS component. Policies must also be improved to ensure that DHS radio users are able to communicate seamlessly with other DHS and federal officials, not to mention state and local officials.
- **Return CFATS to a truly risk-based approach.** A risk-based approach would allow chemical facilities and DHS to focus on the most serious risks. Instead of inflexible regulations that impose large costs on chemical facilities, a risk-based approach would also better respect market principles and allow businesses to manage risks in the most cost-effective manner. This means ensuring that DHS expands the use of ASPs, expedites security plan approvals, and improves risk assessments.
- **Explore alternative funding structures for the FPS.** The GAO recommended comparing alternative funding structures to ascertain the pros and cons of different approaches that include some level of direct appropriation.¹⁷⁰ Inserting a more stable source of income might improve the FPS's budgeting and planning processes as well as improving the way it provides training to its officers. This should be explored by the FPS and the Congressional Research Service.
- **Investigate integration of vetting and case management systems.** Before moving OBIM to another subcomponent, DHS should consider how it could better integrate and update the entire DHS constellation of vetting and case-load systems so that users across DHS are better able to access all the relevant information on an individual.

To fund these activities, the Heritage budget recommends \$3.3 billion for the NPPD.

9. Federal Emergency Management Agency

FEMA had a total budget after rescissions of around \$15.5 billion in FY 2015 and FY 2016, and a request for just over \$16.5 billion for FY 2017.¹⁷¹ As the agency with the largest budget in DHS, FEMA is responsible for three major areas: (1) disaster

relief and preparedness under the Stafford Act; (2) homeland security and emergency preparedness grants; and (3) the National Flood Insurance Program (NFIP). Each of these areas is in desperate need of reform, costing U.S. taxpayers large sums of money and not efficiently serving those who need FEMA. These programs have become political pork that communities and all Members of Congress have come to count on, making changes to these programs difficult. However, it is for just this reason that FEMA needs major reforms, so that these programs can get back to helping people and cease being political footballs and mechanisms for handouts.

Disaster Relief Fund. Throughout most of U.S. history, state and local governments were responsible for responding to nearly all disasters, regardless of the cause. Under President Ronald Reagan, FEMA averaged 28 federal disaster declarations a year.¹⁷² After the passage of the Stafford Act in 1988, this number dramatically changed, with federal disaster declarations steadily rising, so that under President George W. Bush and President Obama, the U.S. has averaged around 130 federal disaster declarations a year.¹⁷³ The result has been that FEMA now responds to a disaster every 2.8 days and has needed ever more money to cover the costs of responding to growing numbers of disasters. The Stafford Act has at least two provisions that are to blame. First, the act shifts at least 75 percent of disaster response costs to the federal government.¹⁷⁴ In the event of a disaster, states normally have to pay for the costs of responding, but if the President declares the disaster worthy of federal assistance, at least 75 percent of response costs are covered by the federal government. The result has been that states now request federal help whenever they can, since it will bring federal dollars. This has created a vicious cycle as states respond to increased federalization of disasters by preparing less and setting less funding aside. As a result, states are less prepared for disasters, they request more government help, and the cycle is perpetuated.

The second problematic provision of the Stafford Act makes it far too easy for states to request disaster assistance. The act vaguely requires that a disaster be “of such severity and magnitude that effective response is beyond the capabilities of the State and the affected local governments and that Federal assistance is necessary,”¹⁷⁵ and that storm-related damages top approximately \$1.40 per capita, which for several states is less than \$1 million.¹⁷⁶ So even

local disasters that are centered in one state and cost as little as \$1 million can be considered federal disasters. This combination of easy-to-acquire federal assistance and the substantial monetary benefit of federal involvement puts FEMA in high demand, leaving it unprepared—both in terms of readiness and money—for truly catastrophic disasters where it is most needed.

Analysis of disaster declarations in 2013 and 2014 indicates that major savings can be had by reforming the Stafford Act. If the Stafford Act's eligibility threshold had been increased to require \$3 per capita in damages with a \$5 million minimum threshold (under which a federal disaster is never declared) and a \$50 million maximum threshold (over which a disaster declaration is always issued), approximately half of all major disaster declarations would not have been issued. According to the cost estimates made to justify a disaster declaration, not issuing disaster declarations for these disasters would save FEMA around \$260 million in 2014 and almost \$400 million in 2013.¹⁷⁷ Of the remaining disasters, the FEMA cost share should be reduced from between 75 percent and 100 percent to 25 percent with a greater cost share for large catastrophes. This system of funding will require states to take responsibility for more localized disasters. It will also ensure that FEMA is able to respond to disasters more effectively, and that it can save funds for catastrophic disasters. For disasters that top \$5 billion, the cost-share provision should gradually increase as the cost of the disaster increases. This gradual increase in cost sharing should be capped at 75 percent once a disaster tops \$20 billion. These thresholds should be properly indexed for inflation to rise over time and ensure that FEMA is most engaged in catastrophic disasters while returning responsibility for smaller disasters to the states.

A potential alternative to the thresholds listed above, which FEMA is currently considering, is the implementation of state and local disaster deductibles. By returning more of the initial costs to the states, states will have an incentive to be better prepared for disasters, and FEMA could reserve more of its focus and funds for larger disasters. This deductible system could even make use of private insurers, who are best positioned to understand the risks in a given state, what the state has done to mitigate those risks, and set the price of a state's insurance premiums and deductible level based on such risk factors. While FEMA

may have the authority to do this via regulation, Congress should also consider how such an effort might improve disaster preparedness and response.

Homeland Security Grants. FEMA is also responsible for administering various homeland security grant programs. These include the State Homeland Security Program (SHSP); the Urban Areas Security Initiative (UASI); Operation Stonegarden (OPSG); various transportation and port security grants; grants for hazard mitigation, such as Flood Mitigation Assistance; grants for firefighters and emergency personnel, such as the Staffing for Adequate Fire and Emergency Response (SAFER); and other preparedness grants, such as the Emergency Management Performance Grants (EMPG).¹⁷⁸

While federal grants to state and local partners may be of value in some cases, the current structure does not adequately prioritize grants based on the risk they are trying to reduce. To the Obama Administration's credit, it has recommended consolidating many of these grants into a new National Preparedness Grant Program that would allot grants in a more risk-based fashion.¹⁷⁹ Grant consolidation should be revisited by Congress and expanded to cover more grant programs. Grants that meet the greatest need in areas of high risk should be prioritized. These grant dollars should not be viewed as another entitlement to send back to each congressional district, but as limited homeland security funding that will alleviate the greatest risks.¹⁸⁰ Failure to prioritize grants weakens security and preparedness, and continues waste and abuse.¹⁸¹

In this process of moving DHS grants to a more risk-based allocation system, the grant programs must be evaluated to see which needs they are meeting and how well they are doing so. Grant programs that are found to be ineffective or unneeded should be cancelled. Heritage Foundation research has found that a variety of firefighter and emergency personnel grants, including SAFER as well as Fire Prevention and Safety (FP&S) grants and Assistance to Firefighter Grants (AFG), do not reduce fire casualties and merely subsidize local fire services.¹⁸² With other more important and more effective areas where such funding could be spent, such grants are a luxury the U.S. cannot afford.

National Flood Insurance Program (NFIP). Originally created in 1968 to help reduce disaster relief payouts, the NFIP has ballooned today into a program that encourages development in high-risk

flood zones. Today, almost all flood insurance is provided by the federal government, because it provides insurance at prices lower than the actuarially fair rate, that is, it subsidizes flood insurance, transferring tax dollars to those who build homes and businesses in flood zones. As a result, when the cost of flooding exceeds the revenue gathered by the program, FEMA ends up requiring a bailout with taxpayers on the hook, which as of 2015 totaled \$23 billion.¹⁸³ By subsidizing building in these zones, the NFIP encourages more people to live in flood zones, increasing the potential losses to the NFIP and the taxpayer.

The Biggert–Waters Flood Insurance Reform Act of 2012 attempted to reduce this effect by making insurance rates more accurately represent the risk of the property and instituting a reserve fund. Congress limited this reform in 2014. Rather than taking additional steps to wind down government involvement in an industry where it does not belong, Congress backtracked and once again instructed FEMA to cap insurance rates and rate increases, thus not correctly accounting for risk, which would allow lower premiums.¹⁸⁴ By undoing and delaying some of the earlier reform, Congress has increased the cost of flood insurance to the average taxpayer. Senator Mike Lee (R–UT) proposed an amendment that would have required owners of second homes and vacation homes to pay higher rates, but Congress rejected his amendment, subsidizing coastal vacation homes at the expense of U.S. taxpayers.¹⁸⁵

As a result, the GAO includes the NFIP in its High-Risk Series, finding that between 2002 and 2013, FEMA missed out on \$11 billion to \$17 billion in net premiums due to federal subsidies.¹⁸⁶ While the GAO points out multiple challenges that FEMA has in administering the NFIP, the GAO also notes that many of the challenges were created by Congress, such as requirements to complete multiple studies in short time frames, mandates that make it impossible for FEMA to run the program sustainably, and multiple changes to the law over the course of several years that stress FEMA’s administrative capability. FEMA is also challenged by the lack of flood-risk information with which to properly determine policies’ full-risk premiums.¹⁸⁷

The NFIP is an inefficient, unnecessary, and costly government intervention into an industry that would otherwise function well. Insurers are capable of assessing risks based on geographic and

weather-based phenomena. Homeowners in areas prone to forest fires, tornados, earthquakes, and other natural disasters can have that added risk built into their policy because insurers can use data on past events, together with home improvements or predicted changes in risk, to price insurance properly. In almost all cases, private flood insurers could conduct the same risk assessment and set prices more in line with the actuarial rate.

Critics of such an approach appeal to the hardship that homeowners in flood-prone zones will face as a result of higher, actuarially sound rates. But this argument is exactly why the NFIP should be terminated. By subsidizing living in higher-risk areas, the NFIP encourages more people to live there—increasing the destruction that individuals face, and increasing the costs to all taxpayers. Why should a farmer in Iowa, a rancher in Texas, or a salesperson in Denver pay for lower insurance rates for someone in Louisiana or Florida? Just as the government should not subsidize or be involved in insurance for tornado or snowstorm damages, FEMA should not be in the business of flood insurance. While there can and should be a transition period to allow private insurance to take the place of federal insurance and to lessen the shock to homeowners, this should be a relatively short period, no longer than four years. The NFIP should be maintained only for the rare cases where private insurance is not available, and it should be done at an actuarially fair price.

Actions for Congress. To stop the over-federalization of disasters, improve the focus of FEMA grants, and improve flood insurance provision in the U.S., Congress should:

- **Reduce the federal share for all FEMA declarations to a 25-percent cost share.** This way, at least three-fourths of the costs of a disaster are borne by the taxpayers living in the state or states where the disaster took place. For catastrophes with a nationwide or widespread regional impact—such as Hurricane Katrina—a relief provision would provide a higher federal cost share if the total costs of the disaster exceeded an inflation-adjusted threshold that began at \$5 billion. Starting at \$5 billion, the cost share would gradually increase as the cost of the disaster increases, maxing out at a 75 percent cost share when a disaster cost more than \$20 billion.

- **Modify the Stafford Act to establish clear requirements that limit the situations in which FEMA can issue declarations.** This should include eliminating some types of disasters from FEMA's portfolio entirely. Another way is to raise the minimum-dollar threshold for requesting disaster declarations. Increasing the threshold to a minimum of \$5 million (and a maximum of \$50 million); increasing the per capita threshold to \$3 per capita; and properly indexing these sums for inflation would significantly reduce the number of events that would warrant a federal disaster declaration. FEMA is currently considering a disaster deductible system for states that could also achieve similar results.
- **Consolidate homeland security and emergency preparedness grant programs and allocate funds in a risk-based manner.** Rather than treating grants as federal dollars that should be spread around, federal grant dollars should be focused on the highest-risk areas and issues. As part of this consolidation, grant programs should be evaluated, and ineffective ones, such as SAFER, FP&S, and AFG, should be cancelled.
- **Begin to transition nearly all users of the NFIP to private insurance.** The NFIP should be wound down. After one year, the NFIP should begin to phase out insurance for lower-risk insured groups (NFIP designations B, C, and X), followed by phasing out NFIP insurance for increasingly high-risk properties (designations A, AE, V, and VE).¹⁸⁸ Within four years, the NFIP should exist only to serve a select few homeowners who are unable to acquire insurance, not because the cost is too high, but because it is not offered in their area. These properties, however, should not be subsidized; these property owners should pay a fee at a rate that is actuarially as fair as possible.

To fund these activities, the Heritage budget recommends \$13.5 billion for FEMA. Specifically:

- **\$1.5 billion for federal assistance**, including cutting ineffective grants like AFG, FP&S, and SAFER, and streamlining all grant programs into one, which will provide grants in a risk-based manner, not based on parochial or political interests.

- **\$5.3 billion for the Disaster Relief Fund**, made possible by the reforms to the Stafford Act that increase eligibility requirements for FEMA funds and decrease the amount of FEMA funds made available, especially for smaller disasters.

10. U.S. Citizenship and Immigration Services

The USCIS had a budget of approximately \$3.2 billion in FY 2014, while in FY 2015 its budget was set to jump to around \$3.77 billion as a result of increased revenue from President Obama's executive action on immigration. With the executive action enjoined, the funding for FY 2016 was only \$3.61 billion, though the President requests just over \$4 billion for FY 2017. The analysis in this *Special Report* assumes that President Obama's executive action will be struck down by the Supreme Court. Due to the USCIS's mostly fee-based funding system, the exact level of revenue, and therefore expenditure, is never entirely clear in advance.

The USCIS is tasked with processing and adjudicating the millions of immigration-related requests made every year. These include work and study visas, E-Verify, green cards or permanent residence, and integration and citizenship. Except for E-Verify, these tasks are paid for with application fees paid by immigrants or those looking to study or work here temporarily. As a result of President Obama's Deferred Action for Childhood Arrivals (DACA) and Deferred Action for Parental Accountability (DAPA) programs, the USCIS is also charged with providing illegal immigrants with the so-called deferred action status, a pseudo-legal status undefined and not authorized anywhere in the Immigration and Nationality Act, but which has come to mean protection from deportation and receiving work-authorization documents and Social Security numbers.

The President's most recent executive action to expand DACA and create DAPA has been the source of considerable controversy as both programs upend the clear meaning of U.S. immigration laws. Rather than enforcing existing laws against illegal presence in the U.S., DACA and DAPA actively work to protect illegal aliens from deportation. Further, despite clear prohibitions of illegal immigrants working in the U.S., these programs turn the prohibitions on their head by authorizing labor and providing Social Security numbers, with all the benefits those entail, including driver's licenses and

tax credits.¹⁸⁹ By not only tolerating, but actively rewarding illegal presence, DAPA and DACA are encouraging *additional* illegal entries, costing U.S. taxpayers more and more.

The result was a threatened slowdown of DHS operations in February 2015, with many Republicans seeking to prevent the USCIS from using any of its funding to carry out the President’s unlawful actions. Congress, however, did not stand its ground, and surrendered to the executive overreach. As a result, the rule of law has been permanently harmed, with the President able to defy congressional action (or inaction) and existing law in furtherance of his own policy preferences. This has created a dangerous precedent for future Presidents, who might use this exact logic to nullify laws with which they disagree, including tax, environmental, labor, privacy, or a host of other laws. Only Federal District Judge Andrew Hanen’s injunction, backed up by the higher courts, stands in the way of this constitutional usurpation of legislative authority.¹⁹⁰

Moving forward, Congress must again stand for its constitutional responsibilities and authority—failure to do so portends greater harm than just this current immigration action. Congress’s only tool in this fight is the power of the purse, and failure to use it condemns it to growing irrelevance and fewer checks on executive power.

Effective and Fair Adjudication of Immigration Benefits. Beyond this current fight over the President’s executive action, the USCIS is in need of other reforms to make it work more efficiently and better adjudicate U.S. immigration laws. While there are large backlogs for various visas due to statutory prescriptions, the USCIS has struggled to adjudicate visas, modernize the visa application system, and prevent abuses of the system.

Kenneth Palinkas, president of the National Citizenship and Immigration Services Council that represents around 12,000 USCIS officials, cited multiple serious problems with the USCIS that should be fixed “before any amnesty proposal is brought forward.”¹⁹¹ He described these problems as:

- “[A] lack of mission support [including] the failure of our software system.”
- “Failure to protect taxpayers from abuses of the welfare system by those granted immigration benefits.”

- “Administrative orders that require us to grant immigration benefits to those who, under law, are not properly eligible” and “approval quotas placed on adjudicators that emphasizes clearing applications more than vetting them.”
- “A management culture that sees illegal aliens and foreign nationals, not US citizens and taxpayers, as the customer. We believe in treating all with respect and always will, but our agency’s focus must be keeping the country safe and secure on behalf of the American people.”¹⁹²

Over the past several years, there have been multiple high-profile examples of improprieties in the way the USCIS adjudicates cases. Before DACA began, a January 2013 report by the IG revealed that USCIS officials were pressuring employees to approve various immigration applications that should have been denied. Furthermore, employees complained of not having enough time to complete interviews of applicants, “leav[ing] ample opportunity for critical information to be overlooked.”¹⁹³

When the USCIS began to process DACA applications, pressure on USCIS employees grew. As with more permanent forms of amnesty, DACA recipients were required to undergo supposedly stringent background checks. E-mails obtained through Freedom of Information Act requests, however, show that several months after the start of DACA, the USCIS moved to a “lean and lite” system of background checks that were not as detailed as the DACA policy itself required. Additionally, the e-mails revealed “managerial pressure not to turn any alien applicant away for lack of ID, including [an] explicit directive in an Oct 3 memo” to this effect.¹⁹⁴

More recently, a multiyear investigation by the DHS IG found that the current Deputy Secretary of DHS and former head of the USCIS, Alejandro Mayorkas, gave special treatment to high-ranking political officials in securing EB-5 visas for investors and job creators. According to the IG, Mayorkas “exerted improper influence in the normal processing and adjudication of EB-5 immigration program benefits.”¹⁹⁵ The most notable beneficiaries of Mayorkas’s improprieties included then-Senate Majority Leader Harry Reid (D-NV), and former Pennsylvania Governor Ed Rendell (D). Anthony Rodham, brother of then-Secretary of State Hillary Clinton, and Terry McAuliffe (D), a former Clinton fundraiser

who is now governor of Virginia, also received special access to EB-5 visas.¹⁹⁶

Despite the ongoing investigation, Mayorkas was promoted by President Obama in 2013. Although the IG found no broken laws, this behavior is not what the U.S. should expect from its senior government officials. Homeland Security Secretary Jeh Johnson doubled down in support of Mayorkas,¹⁹⁷ and Mayorkas himself stated that a “complete and total repudiation of the allegations against [him] is the only correct and just conclusion.”¹⁹⁸

Manipulation of security and screening procedures and pressure on employees to approve applications is obviously wrong. If such behavior occurred in the private sector, it would likely be grounds for legal or regulatory action by the government. Indeed, U.S. Investigations Services, a federal contractor that handles background checks for those seeking employment with the federal government, currently faces legal action from the Department of Justice for taking shortcuts with its background checks on behalf of government customers.¹⁹⁹

Workplace Enforcement of Immigration Laws. The USCIS also handles the E-Verify program that verifies the work authorization of an individual. E-Verify can quickly determine with great accuracy the authenticity of the personal information and credentials offered by new hires. In general, the employer will use a computer to submit certain basic information concerning the employee (name, date of birth, Social Security number) to the government. The information is securely transmitted to DHS and the Social Security Administration, and DHS checks the information to determine whether it corresponds to a U.S. citizen or to a work-eligible immigrant. In most cases, DHS can check and confirm the employee information and transmit a definitive reply to the employer within seconds.

Under federal law, the use of E-Verify is optional for businesses, except for federal government contractors. However, some states, such as Arizona, have made the use of E-Verify mandatory and imposed a series of penalties on employers who knowingly employ “unauthorized aliens.” This includes suspension of the employers’ business licenses, an incentive for complying with the law. The Arizona requirement was upheld by the U.S. Supreme Court in 2011.²⁰⁰ States, despite arguments to the contrary, play a key role in the enforcement of federal immigration law.²⁰¹

In FY 2013, E-Verify automatically confirmed 98.81 percent of workers, with another 0.22 percent confirmed after disputing an initial mismatch, which usually took little more than a week to resolve.²⁰² That leaves just under 1 percent of cases with a non-confirmation.²⁰³ E-Verify’s accuracy has increasingly improved, with one of the most recent studies, from 2012, finding that only 6 percent of final non-confirmations were erroneous.²⁰⁴ Since about 1 percent of cases result in final non-confirmations, this means that approximately 0.06 percent of all E-Verify cases end in erroneous non-confirmations. The system also provides a simple and rapid mechanism for individuals to self-check their own status and discover any errors in their work authorization in order to prevent erroneous non-confirmations.²⁰⁵ On the other hand, estimates from 2009 found that around 3.4 percent of confirmations were erroneous, mostly due to identity fraud.²⁰⁶ Continuing to improve E-Verify by cutting down on errors and tentative non-confirmation-resolution times is important for encouraging business adoption of E-Verify. Additionally, working to combat identity fraud within the program will also improve E-Verify.

Refugees and Security. The USCIS is responsible for adjudicating refugee and asylum claims and admissibility to the U.S. as part of the larger U.S. Refugee Admission Program (USRAP), primarily administered by the State Department. While the U.S. can and should continue to help those in need, security must remain a paramount concern. Following the influx of Syrian refugees and migrants into Europe in 2015, the Obama Administration increased the number of refugees the U.S. would accept from 70,000 in FY 2015 to 85,000 in FY 2016, and a planned 100,000 for FY 2017. The Obama Administration has pledged to reserve at least 10,000 spots for Syrian refugees, a move that drew security concerns, concerns that were heightened following the terrorist attack in Paris, which involved at least one terrorist who entered Europe through the migrant pathway.²⁰⁷ Subsequently, two immigrants who entered the U.S. as refugees have been charged in separate terrorist incidents. Omar Al Harden, who came to the U.S. from Iraq in 2009, is thought to have been planning to bomb two Houston malls,²⁰⁸ while Aws Mohammed Al-Jayab entered the U.S. as a refugee in 2012, and immediately began looking to return to Syria to fight for Islamist terror

organizations. He was successful in getting to Syria in 2013 and returned to the U.S. in 2014.²⁰⁹

Such events have raised real concerns about the U.S. refugee system and its ability to vet refugees. The vetting process includes checking databases across the U.S. government, including those in the Departments of State, Homeland Security, and Defense, the Drug Enforcement Administration, the FBI, the National Counterterrorism Center, as well as Interpol. There is also a USCIS refugee interview conducted by special officers who receive some additional training on country-specific issues. For example, Syrian refugee officers must undergo a one-week training course on Syria-specific issues, including classified information.

In addition, the refugee process requires a Security Advisory Opinion to be completed by the FBI and the intelligence community on many refugee applicants who are considered higher risk. Similarly, interagency checks (IACs) are constantly being done in connection with a wide range of U.S. agencies. In areas of greater concern, as is currently the case with Syria and Iraq, additional scrutiny can be applied to applicants through an enhanced review process that puts additional security and intelligence resources at the disposal of adjudicators.

While the vetting process used by USRAP is the most thorough of any method of entering the U.S., it also faces greater challenges than other methods. As multiple U.S. officials have noted, vetting against intelligence databases can only provide as much information as in the database; that is, if there is little information about an individual in the databases, such screening will not be able to tell refugee officers much.²¹⁰ Since many nations that produce refugees are chaotic, war torn, or have an unfriendly government, the U.S. has limited ways of gathering information with which to vet an individual. The limitations in intelligence vetting puts more pressure on refugee interviewers to corroborate information and detect suspicious behavior.

Given such risks, it is incumbent on the Administration to regularly inform Congress about the risks within the refugee vetting process and how it is mitigating those risks. While the refugee issue is a passionate one, USCIS and Congress should be guided by clear risk assessments that inform continuously refined methods for handling risk.

Challenges to the Visa System: IT and Fraud.

Other failures, most notably of USCIS's IT system and protecting Americans from dangerous individuals

and immigration abuses, are areas ripe for common-sense, good-governance reform. Improving the effectiveness of USCIS should be a priority for any President who wants to better administer the U.S. legal immigration system in order to support the U.S. economy, protect the security of Americans, and make it easier for foreign workers to come here legally.

To work, study, or permanently reside in the U.S., foreign individuals must acquire the appropriate visa. For individuals living around the world, the slowness of the U.S. paper-based system is a hindrance to coming to America. An online system would support the public diplomacy and economy of the U.S. by making it easier for foreigners to come to and remain in the U.S.

The U.S. government, however, has struggled to create an online system to handle most immigration functions. Called a "transformation" of the application system, the Electronic Immigration System (ELIS)—on which the USCIS has \$1.2 billion in sunk costs, well above the original \$500 million originally allocated for the five-year period—missed most major milestones.²¹¹ As of March 2016, users of ELIS could apply for only two of around 90 immigration benefits online, and could pay the \$165 USCIS Immigrant Fee, but not dozens of other potential fees.²¹² DHS is working on rebuilding the system and in early 2014 issued the first of multiple contracts to new vendors.²¹³ As a result, the program will continue to face challenges in the existing system while trying to transition to the new system. Even with this transition, the Inspector General found hundreds of millions of wasted dollars and many continuing problems. While \$1.2 billion have been spent so far on the program, the total life-cycle cost is now estimated at \$3.1 billion. Furthermore, the IG notes that he is "perplexed" and "disappointed" by USCIS's resistance to his investigation and recommendations for improving the program.²¹⁴ It is considered a "medium-risk investment" by DHS's Chief Information Officer.²¹⁵

A simple but important reform that this and future Administrations should undertake is better managing the transformation of USCIS's application system. Other policies, including amnesty, expanded numbers of worker visas, and changes to the number and allocation of green cards, will all increase the number of individuals applying to USCIS, thus adding to USCIS's workload. Without the capability to handle this increased applicant base, security and procedural standards, wait times, and USCIS

budgets will all suffer. Such a reform is important as well as eminently doable if proper attention and oversight are given to the issue. More specifically, DHS should ensure that acquisition best practices, as laid out in a 2011 GAO report on ELIS, are closely followed in order to develop reliable plans for schedules and costs.²¹⁶

While USCIS should make it easier for immigrants to come to the U.S. through an effective Web-based application process, USCIS must also prevent immigration fraud, which opens the U.S. to dangerous individuals and groups as well as additional costs.

A recent example of fraud was uncovered by the House Judiciary Committee, which discovered an unreleased government report that found that as many as 70 percent of asylum cases in 2005 had an indicator of fraud.²¹⁷ While changes in the immigration system have occurred since then, Louis Crocetti, a former head of the Fraud Detection and National Security office at USCIS, said he was “unaware of any immigration benefit fraud assessments, risk assessments, studies, or any other fraud-based research and analysis being performed since the last BFCA [Benefit Fraud and Compliance Assessment] was conducted in 2008,” not just on asylum fraud but on fraud related to all forms of entry.²¹⁸

The GAO studied this issue in 2015 and agreed that “[w]ithout regular assessments of fraud risks, USCIS and EOIR lack reasonable assurance that they have implemented controls to mitigate those risks.”²¹⁹ The GAO also found that much of their case load was handled via paper files, which made fraud investigations logistically difficult. Additionally, even the officers responsible for fraud investigations in the Fraud Detection and National Security Directorate felt they had limited guidance on the issue of fraud. On top of, and perhaps because of, such limited fraud detection, asylum claims have more than doubled between FY 2010 and FY 2014.²²⁰

Those who are granted asylum immediately receive work authorization; the opportunity to acquire derivative asylum visas for a spouse and minor children; and job and English language training, followed by access to a green card after one year and the opportunity to apply for citizenship four years later.²²¹ Asylees are also exempt from “public charge requirements”; that is, they do not have to be economically self-sufficient in order to obtain a green card, and have access to several forms of welfare, including Temporary Assistance for Needy

Families, food stamps, and Medicaid.²²² Such benefits for asylees comport with Americans’ values of human rights and protecting those who cannot return to their home country for fear of persecution and repression. This generosity is not just a moral or principled position, it also furthers American public diplomacy by reinforcing the image of the U.S. as a beacon of freedom.

As can be the case with generosity, however, some take advantage of it. The many benefits the U.S. provides asylees are more than most individuals could ever dream of in their home countries. While the U.S. taxpayers have no problem helping those in need, they do take issue with paying for those who came here fraudulently and then receive redistributed tax dollars.

Despite the costs of fraud, USCIS officials face significant “pressure...to rubber stamp applications.”²²³ Combined with few in-depth fraud investigations occurring within USCIS for any types of visas or requests to enter the U.S., taxpayers are left on the hook for the costs of such fraud, and the security of the U.S. is degraded. In addition to ceasing pressure on USCIS officers to rubber-stamp cases, DHS should reboot credible and public fraud-investigation and fraud-prevention measures.

Patriotic Assimilation Versus Multicultural Partition. USCIS is also responsible for promoting the assimilation of immigrants into U.S. culture and providing citizenship. Under President Obama, this priority has waned into a glorified mechanism to preach political activism that tries to divide immigrants from the rest of U.S. society. As part of his executive action on immigration, President Obama called for a Task Force on New Americans, which created a deeply flawed strategic plan²²⁴ for integrating immigrants. Heritage’s Mike Gonzalez analyzed this plan and found that:

The strategic plan is replete with calls for (1) the “receiving communities” to change so that they can celebrate and accommodate the immigrants’ “diverse linguistic and cultural assets,” rather than the traditional view (and three-century reality) of immigrants becoming Americans over time by assimilating into the nation’s unique culture and developing patriotic sentiments; (2) federal and state government agencies to sanction “diverse cultural practices” rather than maintaining standards and norms that are equally applicable to all citizens; (3) making citizenship easier to attain, rather than the process being a more

meaningful, transformative experience; and (4) “bi-literacy and dual-language learning” in order to “maintain native language proficiency to preserve culture” rather than schools performing their traditional job of promoting a shared cultural experience for all Americans. The plan also (1) accuses schools and agencies that supposedly prevent non-English speakers from having “meaningful access to federally funded programs” of violating the Civil Rights Act’s prohibition of discrimination against protected classes; (2) draws no distinction between citizen and non-citizen, lawful or unlawful resident; and (3) calls for distributing millions of dollars to liberal groups favorable to President Obama.²²⁵

The task force’s recommendations, in other words, make it easier to turn the United States into “more and more a hodgepodge of folks” in the President’s own words—one, moreover, where group differences become entrenched and permanent.²²⁶

This runs against the very essence of America’s history, with leaders as varied as George Washington, Thomas Jefferson, James Madison, Theodore Roosevelt, Woodrow Wilson, Ronald Reagan, and many others proclaiming the importance of assimilation and helping immigrants become Americans.²²⁷

Actions for Congress. To improve USCIS and the adjudication of immigration benefits, Congress should:

- **Reject political influence in the visa-adjudication process.** When the President’s executive actions force USCIS employees to cut corners, and high-ranking politicians are able to wield their influence to obtain green cards for their friends and preferred businesses, the U.S. effectively has a two-tier immigration system—one that serves the well-connected and special-interest groups, and one that deals with everyone else. Basic good governance requires that this sort of corruption and corner cutting not exist. Congress should require the IG to conduct an ongoing investigation into how political preferences and influence are pressuring USCIS employees to bend the rules.
- **Ensure proper vetting in the refugee system and beyond.** To ensure that those entering the U.S. as refugees do not pose a threat to the homeland, Congress should demand that the Administration provide Congress with regular risk assessments on the refugee program developed by the intelligence community. Based on these assessments, the Administration should also provide a plan for managing these risks. Given the potential limitations of intelligence databases, greater training for refugee officials should be considered.
- **Restart comprehensive immigration-fraud evaluations.** The U.S. is a generous nation that provides many people with immigration benefits, but there are too many who abuse the system. Given the value of U.S. visas and citizenship, the U.S. should do much more to investigate fraud, both on a case-by-case basis as well as through more comprehensive risk assessments and investigations.
- **Strengthen E-Verify against identity theft.** E-Verify prevents unauthorized workers from being employed, but one flaw with the system is that those using legitimate Social Security numbers acquired through identity theft can be authorized. The Social Security Administration should be required to work with the E-Verify system to identify cases where Social Security numbers are being used in multiple places or in suspicious ways.
- **Reform the USCIS’s funding mechanism.** To help USCIS engage more in fraud prevention, acquire better IT systems such as ELIS, and improve other administrative functions, the USCIS funding model should be changed. Currently, only E-Verify is funded by appropriations. Congress should move administrative parts of the agency to more regular appropriations to ensure that the funding of basic functions are dependent on the level of visa revenues.
- **Promote real assimilation.** Becoming an American should be a deeply meaningful experience that instills immigrants with love of America and her values. Current integration measures portray citizenship as little more than a legal right to a U.S. passport. *This must change.* USCIS must retool its integration efforts and not focus on multiculturalism, diversity, and activism as the desired values, but on patriotism, American principles, and civic education.

To fund these activities, the Heritage budget recommends \$3.7 billion for USCIS.

11. Federal Law Enforcement Training Centers

The Federal Law Enforcement Training Centers' (FLETC) FY 2016 budget of \$244 million fell slightly from the FY 2014 and FY 2015 levels of \$258 million, with President Obama requesting \$242 million for FY 2017. The FLETC are a unique part of DHS that is entirely dedicated to training federal, state, local, and even international law enforcement, in a variety of skills and situations. Given the large size of the U.S. and that, as of 2008, it had around 810,000 state and local law enforcement officers (with more than 400,000 support staff),²²⁸ the FLETC play an important role in preparing these officers and staff for the future.

With primary facilities in Georgia, South Carolina, New Mexico, and outside Washington, DC, as well as other partner and support facilities in Los Angeles, Washington, DC, and Orlando, the FLETC provide training in areas as varied as:

- Marksmanship,
- Active shooter threats,
- Forensics,
- Medical care,
- Vessel and boat boarding,
- Computer network investigation,
- Legal and use of force,
- Drug law enforcement,
- Critical infrastructure security,
- Non-lethal weapons, and
- Vehicle and driving training.²²⁹

In addition to training law enforcement officers in these areas, FLETC also offer several “train the trainer” programs that improve other training efforts across the U.S. To better serve the law enforcement

community, the FLETC's Online Campus provides law enforcement training resources via the Internet. For FY 2015, the FLETC reported that it “trained 65,341 law enforcement personnel, including 7,344 state and local law enforcement officers and 1,286 international law enforcement personnel.”²³⁰

Despite the importance of training at the FLETC and other DHS subcomponents, the IG found that DHS has consistently failed to report training costs. The IG found that of the approximately \$1.4 billion allocated for training in the FY 2014 budget, DHS had only reported \$1.9 million to OPM as required and the DHS CFO could only account for \$267.6 million.²³¹ This is not the first time DHS has been criticized for such management practices, as concerns have existed since 2003, including the 2015 GAO High Risk report. While the FY 2016 appropriation includes funding for a modernized finance system and other reporting policy changes, Congress must demand that DHS be able to complete basic reporting requirements.

Actions for Congress. Since state and local law enforcement officers are often the first to respond to and deal with a crisis, such as an active shooter, DHS should expand “train the trainer” programs and direct the training of state and local officers. To continue and further the FLETC mission, the Heritage budget recommends \$300 million, which should be spent on expanding operations. Additionally, DHS has had multiple studies and working groups that studied training expenditures and efficiencies, but has failed to act on such studies' recommendations.²³² DHS should be required to further integrate training centers, looking for training facilities operated by other agencies that could be consolidated and operated by the FLETC.²³³

12. Science and Technology Directorate, Domestic Nuclear Detection Office, and Office of Health Affairs

The Science and Technology Directorate (S&T) received just over \$1.2 billion in FY 2014 and \$1.1 billion in FY 2015, falling to \$787 million FY 2016, with President Obama's budget request for FY 2017 seeking around \$760 million. This significant decrease is due to the completion of funding for the new Bio-Agro Defense Facility in Kansas. S&T is the primary research-and-development arm of DHS, but as the Congressional Research Service concluded, “despite several restructurings and close congressional oversight, the S&T Directorate continues to face difficulties in meeting congressional expectations.”²³⁴

S&T Organization. S&T is broken up into multiple groups, each with a different focus:

- The First Responder’s Group conducts R&D to provide the emergency preparedness and response community with products specific to their missions;²³⁵
- The Research and Development Partnership Group works with federal, academic, and private laboratories on R&D activities and projects;²³⁶
- The Homeland Security Advanced Research Projects Agency (HSARPA) develops advanced technologies and capabilities to better equip and prepare homeland security officials in the field;²³⁷ and
- Other offices, including the Capability Development Support Group, which defines mission needs, finds cost-effective solutions, and evaluates solution outcomes.²³⁸

The Congressional Research Service notes that these groups have no statutory basis and have been reshuffled regularly, usually with every new Under Secretary for S&T.²³⁹

Too Many Research Programs, Not Enough Focus. Despite these reorganizations, one significant problem with S&T research is that it does not adequately meet mission needs or benefit national security.²⁴⁰ According to the GAO, DHS components that were surveyed “consistently said they were aware of few or no products that S&T had transitioned from one of S&T’s R&D projects to their respective components.”²⁴¹ As a result, S&T customers are likely to view S&T as not meeting end-user needs.²⁴² In the descriptions for the various parts of S&T, it is clear that the department is working to align research programs with mission needs, but S&T will need to consistently ensure that research programs are properly aligned with DHS-component needs.

The current Under Secretary, Dr. Reginald Brothers, has sought to address this issue by reducing the overall number of research programs in order to ensure that more attention is paid to the remaining programs. Under Brothers, S&T also started a pilot program that assigns S&T researchers to components’ laboratories in order to give researchers a better understanding of what is occurring at, and what

is needed by, that component.²⁴³ It is not yet clear that these changes will be sufficient to deal with the problem, but seeking to better understand and focus on the needs of DHS components, S&T’s primary customer, is a step in the right direction.

S&T and the Private Sector. A related issue with which S&T has struggled is coordinating research within DHS and with the private sector. As with many government research activities, there are often concerns that government research is duplicating work by other government organizations or the private sector. Responsible for research within DHS, only in September 2014 did S&T define what “research and development” means for the department,²⁴⁴ bringing it in line with the Office of Management and Budget’s definitions.²⁴⁵ Poor coordination of research activities not only harms the usefulness of end products in meeting mission needs, but also “makes it difficult to oversee activities across the department” and appropriately allocate resources.²⁴⁶ In fact, the GAO found in 2012 that S&T did not know how much all DHS components were spending on R&D.²⁴⁷ S&T has developed a definition of R&D and is working to encourage interagency communication and now must take additional steps to track R&D spending and ensure that spending is coordinated and not unnecessarily duplicative.²⁴⁸

S&T must do more to ensure that it does not duplicate the work of the private sector. The U.S. private sector is constantly striving to develop new products that are of interest to DHS personnel or state and local officials. From private cybersecurity and technology innovations to disaster response equipment, the U.S. private sector is the most powerful force for innovation in the world. S&T, however, may not always know of technologies or products available in the private sector that could meet DHS’s general needs or specific requirements. As a result, S&T’s office of Research and Development Partnerships has begun focusing on what it calls “technology foraging,” which seeks out existing or emerging technologies that could be adapted to meet DHS’s needs. This effort should be expanded as it costs the government less and will likely be faster than brand-new research and development.

SAFETY Act. A way to further encourage private-sector innovation is to expand the Support Anti-Terrorism by Fostering Effective Technologies Act. Passed as part of the Homeland Security Act of 2002, the SAFETY Act provides liability protection

for sellers of qualified anti-terrorism technologies (QATTs) whose products or services may help prevent or mitigate a terrorist attack.²⁴⁹ This protection is necessary so that the private sector does not fear being sued if its products are deployed and a terrorist attack occurs anyway.

The SAFETY Act provides different levels of certification to different products depending on their effectiveness. QATT certifications can be extended to products and services such as:

- Threat and vulnerability assessment services,
- Detection systems,
- Blast mitigation materials,
- Screening services,
- Sensors and sensor integration,
- Threatening object detectors,
- Decision support software,
- Security plans/services,
- Crisis management systems, and
- Venue security.²⁵⁰

The SAFETY ACT has resulted in certification of hundreds of technologies and services since its creation, increasing innovation and security. The U.S., however, is not the only country producing advanced and novel security services and technologies. By working with other countries, the U.S. can benefit from more products and also increase the market for U.S. products. To make this happen, the U.S. should work with allies and partners on a bilateral basis to extend reciprocal liability protection regimes.²⁵¹

A good potential pilot country for this expansion of the SAFETY Act would be Israel, which has a vibrant security industry, a relatively similar legal system, and a small economy. After working out the details and seeing how the pilot program works, the U.S. could then consider expanding the program to other allies, such as Canada and Great Britain.

Employee Morale. Another issue with which S&T has struggled is employee morale. S&T was tied with

ICE as the worst office in the federal government for which to work, according to the Partnership for Public Service's annual survey.²⁵² Morale and workplace satisfaction issues seem to be at least somewhat connected to S&T's larger performance problems. Be it innovation, teamwork, strategic management, performance-based rewards, empowerment by leaders, or how well employees' skills match their mission—employees all expressed significant dissatisfaction with how S&T handles these issues. S&T employees expressed negative feelings for other non-performance or mission-oriented issues, such as pay and support for diversity.

Domestic Nuclear Detection Office. Currently, the Domestic Nuclear Detection Office (DNDO), as its name implies, focuses on domestic nuclear forensics and detection capabilities. With a budget of approximately \$347 million in FY 2016, the DNDO works with partners across the government as well as the private sector and academia to increase and improve the research, development, and use of nuclear-radiation-detection technologies. To this end, it has been successful in working with the CBP to ensure that 99.8 percent of incoming U.S. sea cargo containers are screened through a radiation portal before leaving the port. The DNDO also conducts various exercises with other agencies, such as law enforcement, to improve the use of detection equipment. The DNDO is pressing forward with a new Securing the Cities program intended "to enhance the capability of all our partners to detect and interdict dangerous radiological and nuclear weapons or materials in major metropolitan areas."²⁵³ The DNDO faced some challenges in the past but more recently has generally received bipartisan praise.²⁵⁴ Despite its successes, the DNDO could improve its R&D by more explicitly tying its research investments to those gaps that it seeks to close.²⁵⁵

Office of Health Affairs. Another similar R&D-focused organization is the Office of Health Affairs (OHA), which focuses on biological and chemical incidents. With its budget of \$125 million in FY 2016, the OHA's main program, BioWatch, detects biological agents in high-risk areas, such as subways,²⁵⁶ but its third generation was cancelled due to a price tag as high as \$3 billion and technical challenges.²⁵⁷ Despite these challenges, the need for early detection of a biological agent remains real and the OHA is left running the legacy BioWatch second generation. Other than a few planning and advisory roles, the OHA currently lacks a clear vision for what its future should entail.

To this end, DHS is considering reorganizing the way it manages R&D. Currently, other organizations, including the DNDO, the OHA, the Coast Guard, and the CBP, also conduct research that is supposed to be coordinated by S&T. Past reorganization efforts have considered moving the DNDO and the OHA into S&T to benefit from greater efficiencies of a single R&D organization. Another idea, proposed by DHS, is to merge the DNDO, the OHA, and possibly parts of other organizations into a Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE) Directorate. However, given the challenges that the S&T currently faces, a reorganization is not necessarily the solution. Better policy and formal coordination are less disruptive fixes to the problems facing S&T right now.

As for a CBRNE-focused organization, it may seem appealing on its face, but it overlooks a more serious need for the U.S. government to do a far better job coordinating CBRNE functions. The Environmental Protection Agency,²⁵⁸ the Department of Health and Human Services,²⁵⁹ the Department of Defense,²⁶⁰ and other agencies share responsibilities with DHS for preparing and responding to different CBRNE incidents. Across the government, the U.S. needs to take the possibility of a CBRNE disaster more seriously, establishing resources, creating strategies and policies that cut across organizational lanes, and establishing a clearer coordinating authority and structure. While DHS has a significant role to play in such reforms, such reform is beyond the scope of this *Special Report*.

Actions for Congress. While the leaders of DHS's R&D organizations have taken some positive steps toward improvement, their work is far from over.²⁶¹ Morale improvement, coordination of research with mission needs, and greater department-wide coordination of research must be priorities. To meet these objectives, Congress and the Administration should:

- **Develop clear policies for overseeing R&D.** With S&T just now defining R&D, S&T and other DHS components must properly report and account for spending on their research activities. This should feed into a mechanism for tracking R&D projects and total expenditures. While S&T has taken preliminary steps to assign roles and responsibilities for coordination of R&D projects, Congress should oversee these new guidelines to ensure that relevant agencies are fulfilling their responsibilities.
- **Reject pork in R&D missions.** R&D is a common area in which Congress mandates certain pork-barrel projects that benefit parochial interests in Members' districts regardless of the wisdom of such an investment. While Congress can and should oversee spending efforts, it should not insert political and parochial interests to the detriment of actual R&D.
- **Focus on primary customers—DHS components.** While S&T's efforts can have benefits for state and local governments and the private sector, S&T should focus on meeting the needs of DHS components first and foremost.
- **Formalize relationships between S&T and other components.** To better coordinate research and meet component needs, Congress should more formally connect S&T with research and requirement-setting activities that define what exactly is needed from S&T research. At a high level, this means the creation of a formal oversight council or process to ensure that S&T and relevant parties share visibility and understanding of research projects. At a lower level, this means expanding initiatives, such as Apex programs, which involve integrating component staff in the S&T R&D process to increase research usefulness to end-users.²⁶²
- **Expand the SAFETY Act.** One way to support the development of products that support end-user needs is to expand the SAFETY Act, since profit is a good incentive for developing products and services that meet user needs. By expanding the SAFETY Act's protections in a reciprocal nature with other nations, the U.S. will have access to even more lifesaving technologies. Congress should start a pilot program with a willing ally, such as Israel, to work out the details.

To fund these activities, the Heritage budget recommends \$750 million for S&T. Heritage also recommends:

- \$350 million for the Domestic Nuclear Detection Office, and
- \$130 million for the Office of Health Affairs.

Making DHS Work for America

As threats of terrorism, cyber espionage, and cyberattacks grow, the U.S.'s immigration system continues to erode, trade and travel continue to expand, and natural disasters remain an ever-present reality, the U.S. must demand significant reform to the Department of Homeland Security. Such reforms are necessary to ensure the safety and security of the U.S. homeland—and they must take place amidst the reality that the current level of federal spending is unsustainable. With annual deficits in the hundreds of billions of dollars in addition to \$18 trillion in federal debt, and with entitlements, welfare programs, and interest payments consuming two-thirds of the budget in FY 2014 and growing, all spending must be carefully reviewed. While reforms to the main drivers of U.S. debt—entitlement and welfare programs—are long past due, it is crucial that Congress focus on and prioritize DHS spending.

The Heritage Foundation's alternative budget is both fiscally responsible and makes the U.S. more secure and prepared by focusing on DHS's priorities. Reforms to FEMA can save money immediately and other reforms to FEMA, the TSA, and other agencies will yield longer-term savings. Some of the funding saved through reforms will be redirected to priorities such as the Coast Guard, cybersecurity, counterterrorism, and immigration-law enforcement. This budget also does its part to fix the U.S.'s fiscal woes by reducing spending by about \$2 billion from FY 2016, a 3 percent decrease.

While cutting spending is rarely a popular idea, these cuts redirect funding to more critical activities and, combined with the policy reforms in this *Special Report*, improve DHS operations. In other words, if implemented, these recommendations and funding priorities will do more with less. The Heritage budget does its part to improve the U.S.'s fiscal health and make America safer and more secure.

These reforms cannot wait.

Endnotes

1. The numbers used in this report are drawn from the Consolidated Appropriations Act, 2016, P.L. 114-113; the associated explanatory statement by House Appropriations Chairman Hal Rogers (R-KY); and the President's budget requests. Consolidated Appropriations Act, 2016, P.L. 114-113, <https://www.congress.gov/bill/114th-congress/house-bill/2029/text> (accessed April 29, 2016); "Division F- Department of Homeland Security Appropriations Act 2016," U.S. House of Representatives, <http://docs.house.gov/meetings/RU/RU00/20151216/104298/HMTG-114-RU00-20151216-SD007.pdf> (accessed April 29, 2016); Department of Homeland Security, *Congressional Budget Justification, FY 2017*, <https://www.dhs.gov/publication/congressional-budget-justification-fy-2017> (accessed April 29, 2016); and Department of Homeland Security, *Budget-in-Brief, Fiscal Year 2017*, https://www.dhs.gov/sites/default/files/publications/FY2017_BIB-MASTER.pdf (accessed April 29, 2016).
2. While some of this funding may end up being spent by other sub-components and offices, all of it will be disbursed by the Secretary.
3. U.S. Government Accountability Office, "Progress Made, but Work Remains in Strengthening Acquisition and Other Management Functions," GAO-16-507T, February 11, 2015, <http://www.gao.gov/assets/680/675827.pdf> (accessed March 24, 2016).
4. Ibid.
5. Ibid.
6. Ibid.
7. U.S. Office of Personnel Management, Planning and Policy Analysis, *Federal Employee Viewpoint Survey Results*, October 16, 2016, http://www.fedview.opm.gov/2015FILES/2015_FEVS_Gwide_Final_Report.PDF (accessed April 13, 2016).
8. The Best Places to Work in the Federal Government, "Department of Homeland Security," 2015, <http://bestplacestowork.org/BPTW/rankings/detail/HS00> (accessed March 10, 2016).
9. The Aspen Institute, "Task Force Report on Streamlining and Consolidating Congressional Oversight of the U.S. Department of Homeland Security," The Annenberg Foundation Trust at Sunnyslands, September 2013, <http://www.aspeninstitute.org/sites/default/files/content/docs/pubs/Sunnyslands%20report%2009-11-13.pdf> (accessed July 16, 2015).
10. Ibid.
11. Jessica Zuckerman, "Politics Over Security: Homeland Security Congressional Oversight in Dire Need of Reform," Heritage Foundation *Issue Brief* No. 3722, September 10, 2012, <http://www.heritage.org/research/reports/2012/09/homeland-security-congressional-oversight-in-dire-need-of-reform>.
12. Eugene Scott, "FBI Director: U.S. Facing Greatest Threat from Terrorist Groups Since 9/11," CNN, December 9, 2015, <http://www.cnn.com/2015/12/09/politics/terrorist-threats-fbi-director-9-11/> (accessed April 13, 2016).
13. J. J. Green, "Target USA: DNI Jim Clapper Reveals Unprecedented Threats Facing U.S.," WTOP, February 1, 2016, <http://wtop.com/j-j-green-national/2016/02/target-usa-dni-jim-clapper-reveals-unprecedented-threats-facing-u-s/> (accessed April 13, 2016).
14. Permanent Subcommittee on Investigations, "Federal Support for and Involvement in State and Local Fusion Centers," Committee on Homeland Security and Governmental Affairs, U.S. Senate, October 3, 2012.
15. Brian Jenkins, Andrew Liepman, and Henry H. Willis, "Identifying Enemies Among Us," RAND Corporation, 2014, http://www.rand.org/content/dam/rand/pubs/conf/proceedings/CF300/CF317/RAND_CF317.pdf (accessed April 10, 2015).
16. Department of Homeland Security, "Fusion Center Locations and Contact Information," January 9, 2015, <http://www.dhs.gov/fusion-center-locations-and-contact-information> (accessed April 10, 2015), and Federal Bureau of Investigation, "Protecting America from Terrorist Attack," http://www.fbi.gov/about-us/investigate/terrorism/terrorism_jtfts (accessed on April 9, 2015).
17. Department of Homeland Security, "Homeland Security Information Network Improvements and Challenges," OIG-13-98, June 2013, https://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-98_Jun13.pdf (accessed April 29, 2016).
18. Department of Homeland Security, "HSIN 2014 Annual Report," http://www.dhs.gov/sites/default/files/publications/HSIN-2014-Annual-Report_0.pdf (accessed April 29, 2016).
19. U.S. Government Accountability Office, "DHS Intelligence Analysis: Additional Actions Needed to Address Analytic Priorities and Workforce Challenges," GAO-14-397, June 4, 2014, <http://www.gao.gov/products/GAO-14-397> (accessed April 10, 2015).
20. The Best Places to Work in the Federal Government, "Intelligence and Analysis (DHS)," 2015, <http://bestplacestowork.org/BPTW/rankings/detail/HS07> (accessed March 10, 2016).
21. Department of Homeland Security, "Fiscal Year 2015 Homeland Security Grant Program," http://www.fema.gov/media-library-data/1438021101390-ce3bbdde8b84b174b8212fcd7aaa5c3/FY_2015_HSGP_Fact_Sheet_Allocations.pdf (accessed July 30, 2015).
22. James Jay Carafano and Jessica Zuckerman, "Maritime Cargo Scanning Folly: Bad for the Economy, Wrong for Security," Heritage Foundation *WebMemo* No. 3481, February 2, 2012, <http://www.heritage.org/research/reports/2012/02/maritime-cargo-port-security-and-the-100-percent-screening-mandate>.
23. Vivian C. Jones and Lisa Seghetti, "U.S. Customs and Border Protection: Trade Facilitation, Enforcement, and Security," Congressional Research Service *Report* R43014, May 18, 2015, <http://fas.org/sgp/crs/homsec/R43014.pdf> (accessed July 17, 2015). DHS is scanning 99.8 percent of sea containers through radiation portals in the U.S.—but this does not include imaging, which is equally important.

24. Agricultural Retailers Association et al., "Letter to Secretary Jeh Johnson," June 2, 2014, <https://nrf.com/sites/default/files/Documents/100%20Scanning%20Industry%20Letter%20to%20Secretary%20Jeh%20Johnson%20Final%20060214%20%284%29.pdf> (accessed June 2, 2015), and Frederic Carlier, "Global Logistic Chain Security: Economic Impacts of the US 100% Container Scanning Law," University of Le Havre Study Commissioned by the World Customs Organization (WCO), June 2008, <http://www.wcoomd.org/en/media/newsroom/2008/june/-/media/5F04492F60C6460BB269478A0F2A80AD.ashx> pdf (accessed May 5, 2015).
25. Steven P. Bucci and David Inserra, "Biometric Exit Improvement Act: Wrong Solution to Broken Visa and Immigration System," Heritage Foundation *Issue Brief* No. 4064, October 8, 2013, <http://www.heritage.org/research/reports/2013/10/biometric-exit-improvement-act-and-the-broken-visa-and-immigration-system>.
26. Steven P. Bucci, "Visa Waiver Program Improves Security," testimony before the Subcommittee of Border and Maritime Security, Committee on Homeland Security, U.S. House of Representatives, March 17, 2015, <http://www.heritage.org/research/testimony/2015/visa-waiver-program-improves-security>.
27. David Inserra, "Congress Should Expand Trusted Traveler Programs and Private Airport Screeners," Heritage Foundation *Issue Brief* No. 4359, March 3, 2015, <http://www.heritage.org/research/reports/2015/03/congress-should-expand-trusted-traveler-programs-and-private-airport-screeners>.
28. U.S. Department of Homeland Security, "Comparison Chart," December 4, 2014, <http://www.dhs.gov/comparison-chart> (accessed March 2, 2015).
29. U.S. Customs and Border Protection, "Trusted Traveler Programs," 2015, <http://www.cbp.gov/travel/trusted-traveler-programs> (accessed March 2, 2015).
30. Jessica Zuckerman, "Global Entry Reciprocity: Creating a Trusted Travel Superhighway," Heritage Foundation *Issue Brief* No. 3753, October 11, 2012, <http://www.heritage.org/research/reports/2012/10/global-entry-reciprocity-and-us-share-of-overseas-travel>.
31. David Inserra, "Children Illegally Crossing the U.S. Border: Responding Requires Policy Changes," Heritage Foundation *Issue Brief* No. 4248, July 15, 2014, <http://www.heritage.org/research/reports/2014/07/children-illegally-crossing-the-us-border-responding-requires-policy-changes>.
32. Best Places to Work in the Federal Government, "Customs and Border Protection (DHS)," 2015, <http://bestplacestowork.org/BPTW/rankings/detail/HS03> (accessed March 10, 2016).
33. David Inserra, "Ten-Step Checklist for Revitalizing America's Immigration System: How the Administration Can Fulfill Its Responsibilities," Heritage Foundation *Special Report* No. 160, November 3, 2014, <http://www.heritage.org/research/reports/2014/11/ten-step-checklist-for-revitalizing-americas-immigration-system-how-the-administration-can-fulfill-its-responsibilities>.
34. Secure Fence Act of 2006, P.L. 109-367, <http://www.gpo.gov/fdsys/pkg/PLAW-109publ367/pdf/PLAW-109publ367.pdf> (accessed September 23, 2014).
35. U.S. Immigration and Customs Enforcement, "Civil Immigration Enforcement: Priorities for the Apprehension, Detention, and Removal of Aliens," Policy No. 10072.1, March 2, 2011, <http://www.ice.gov/doclib/news/releases/2011/110302washingtondc.pdf> (accessed May 13, 2016); U.S. Immigration and Customs Enforcement, "Exercising Prosecutorial Discretion Consistent with the Civil Immigration Enforcement Priorities of the Agency for the Apprehension, Detention, and Removal of Aliens," Policy No. 10075.1, June 17, 2011, <http://www.ice.gov/doclib/secure-communities/pdf/prosecutorial-discretion-memo.pdf> (accessed May 13, 2016); and U.S. Immigration and Customs Enforcement, "Prosecutorial Discretion: Certain Victims, Witnesses, and Plaintiffs," Policy No. 10076.1, June 17, 2011, <http://www.ice.gov/doclib/secure-communities/pdf/domestic-violence.pdf> (accessed May 13, 2016).
36. *Ibid.*, and John Malcolm, "President Obama's Executive Action on Immigration Sets a Dangerous Precedent," Heritage Foundation *Issue Brief* No. 4313, December 5, 2014, <http://www.heritage.org/research/reports/2014/12/president-obamas-executive-action-on-immigration-sets-a-dangerous-precedent>.
37. Department of Homeland Security, "DHS Releases End of Fiscal Year 2015 Statistics," December 22, 2015, <http://www.dhs.gov/news/2015/12/22/dhs-releases-end-fiscal-year-2015-statistics> (accessed April 13, 2016).
38. Immigration and Customs Enforcement, "FY 2015 ICE Immigration Removals," Immigration and Customs Enforcement, 2015, <https://www.ice.gov/removal-statistics> (accessed April 13, 2016).
39. Center for Immigration Studies, "Interior Enforcement Disintegrates Further in 2015," December 2015, <http://cis.org/Interior-Enforcement-2015-Deportations> (accessed April 13, 2016).
40. The Best Places to Work in the Federal Government, "Immigration and Customs Enforcement (DHS)," 2015, <http://bestplacestowork.org/BPTW/rankings/detail/HS06> (accessed April 13, 2016).
41. U.S. Department of Justice, Office of Planning, Analysis, & Technology, "FY 2015 Statistics Yearbook," April 2016, <https://www.justice.gov/sites/default/files/pages/attachments/2016/04/08/fy15syb.pdf> (accessed May 6, 2016).
42. Brandon Judd, statement before the Subcommittee on National Security, Committee on Oversight and Government Reform, U.S. House of Representatives, March 23, 2015, <https://oversight.house.gov/wp-content/uploads/2016/03/2016-03-23-Judd-Testimony-NBPC.pdf> (accessed April 25, 2016).
43. Elizabeth Slattery, "Supreme Court Immigration Showdown: Why States Can Enforce Immigration Laws," Heritage Foundation *Issue Brief* No. 3573, April 20, 2012, <http://www.heritage.org/research/reports/2012/04/supreme-court-and-immigration-policy-why-states-can-enforce-immigration-laws>.

**CONGRESS MUST RE-SET DEPARTMENT OF HOMELAND SECURITY PRIORITIES:
AMERICAN LIVES DEPEND ON IT**

44. U.S. Immigration and Customs Enforcement, "Fact Sheet: Delegation of Immigration Authority Section 287(g) Immigration and Nationality Act," <http://www.ice.gov/news/library/factsheets/287g.htm> (accessed October 2, 2014).
45. U.S. Immigration and Customs Enforcement, "Secure Communities," http://www.ice.gov/secure_communities/ (accessed August 28, 2014).
46. Ibid.
47. U.S. Immigration and Customs Enforcement, Office of the Director, "ICE Response to the Task Force on Secure Communities Findings and Recommendations," April 27, 2012, <http://www.ice.gov/doclib/secure-communities/pdf/hsac-sc-taskforce-report.pdf> (accessed September 2, 2014).
48. Ibid.
49. Jeh Johnson, "Secure Communities," Department of Homeland Security Memorandum to Thomas S. Winkowski, Acting Director, ICE, November 20, 2014, http://www.dhs.gov/sites/default/files/publications/14_1120_memo_secure_communities.pdf (accessed July 20, 2015).
50. Department of Homeland Security, Office of the Chief Financial Officer, *U.S. Department of Homeland Security Annual Performance Report: FY2012-2014*, April 10, 2013, p. 1414, <http://www.dhs.gov/sites/default/files/publications/MGMT/DHS-%20Annual%20Performance%20Report%20and%20Congressional-Budget-Justification-FY2014.pdf> (accessed August 28, 2014).
51. Department of Homeland Security, *Budget-in-Brief: Fiscal Year 2014*, p. 130, <http://www.dhs.gov/sites/default/files/publications/MGMT/FY%202014%20BIB%20-%20FINAL%20-508%20Formatted%20%284%29.pdf> (accessed August 28, 2014).
52. News release, "Statement by Secretary Napolitano on DOJ's Findings of Discriminatory Policing in Maricopa County," Department of Homeland Security, December 15, 2011, <https://www.dhs.gov/news/2011/12/15/secretary-napolitano-dojs-findings-discriminatory-policing-maricopa-county> (accessed August 28, 2014).
53. Jeremy Duda, "Homeland Security Revokes 287(g) Agreements in Arizona," *Arizona Capitol Times*, June 25, 2012, <http://azcapitoltimes.com/news/2012/06/25/homeland-security-revokes-287g-immigration-check-agreements-in-arizona/> (accessed August 28, 2014).
54. Lev J. Kubiak, "Crisis of Confidence: Preventing Terrorist Infiltration Through U.S. Refugee and Visa Programs," testimony before the Committee on Homeland Security, U.S. House of Representatives, February 3, 2016, <http://docs.house.gov/meetings/HM/HM00/20160203/104344/HHRG-114-HM00-Wstate-KubiakL-20160203.pdf> (accessed April 13, 2016).
55. David Inserra, "Congress Should Expand Trusted Traveler Programs and Private Airport Screeners," Heritage Foundation *Issue Brief* No. 4359, March 3, 2015, <http://www.heritage.org/research/reports/2015/03/congress-should-expand-trusted-traveler-programs-and-private-airport-screeners>, and "TSA PreCheck®," Transportation Security Administration, <https://www.tsa.gov/tsa-precheck> (accessed May 9, 2016).
56. Transportation Security Administration, "Participation in TSA PreCheck," November 20, 2014, <http://www.tsa.gov/tsa-precheck/participation-tsa-precheck%20%284%29> (accessed March 2, 2015).
57. News release, "TSA PreCheck Reaches Milestone: More Than 1 Million Travelers Enrolled," Transportation Security Administration, January 13, 2016, <http://www.tsa.gov/press/releases/2015/03/24/tsa-precheck-reaches-milestone-more-1-million-travelers-enrolled> (accessed March 10, 2016).
58. Government Accountability Office, "Aviation Security: Rapid Growth in Expedited Passenger Screening Highlights Need to Plan Effective Security Assessments," GAO-15-150, December 12, 2014, <http://www.gao.gov/products/GAO-15-150> (accessed March 2, 2015); Department of Homeland Security, "Security Enhancements Needed to the PreCheck Initiative," OIG-15-29, January 28, 2015, http://www.oig.dhs.gov/assets/Mgmt/2015/OIG_15-29_Feb15.pdf (accessed March 2, 2015); and Christian Beckner, "Risk-Based Security and the Aviation System: Operational Objectives and Policy Challenges," Center for Cyber and Homeland Security at George Washington University, *Issue Brief* No. 2015-02, January 2015, <https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/GW%20CCHS%20-%20Risk-Based%20Security%20and%20the%20Aviation%20System%20-%20Jan%202015%281%29.pdf> (accessed March 2, 2015).
59. Harriet Baskas, "New TSA Chief Vows to Improve 96% Failure Rate on Weapons Detection," NBC News, July 30, 2015, <http://www.nbcnews.com/business/travel/new-tsa-chief-vows-improve-96-failure-rate-weapons-detection-n401011> (accessed July 30, 2015), and Lori Aratani, "Change in TSA Screening May Mean Longer Waits at TSA Checkpoints," *The Washington Post*, October 29, 2015, <https://www.washingtonpost.com/news/dr-gridlock/wp/2015/10/29/no-more-cutting-the-line-at-tsa-screening/> (accessed May 9, 2016).
60. Department of Homeland Security, "Cargo Screening," September 19, 2014, <http://www.dhs.gov/cargo-screening> (accessed May 5, 2015).
61. Lisa Seghetti, "Border Security: Immigration Inspections at Ports of Entry," Congressional Research Service *Report* R43356, January 26, 2015, <https://fas.org/sgp/crs/homsec/R43356.pdf> (accessed July 20, 2015).
62. Jena Baker McNeill, "Air Cargo Security: How to Keep Americans Secure without Harming the Economy," Heritage Foundation *Backgrounder* No. 2422, June 21, 2010, <http://www.heritage.org/research/reports/2010/06/air-cargo-security-how-to-keep-americans-secure-without-harming-the-economy>.
63. John Roth, "Transportation Security, Are Our Airports Safe?" testimony before the Committee on Oversight and Government Reform, U.S. House of Representatives, May 13, 2015, https://www.oig.dhs.gov/assets/TM/2015/OIGtm_JR_051315.pdf (accessed May 14, 2015).
64. Ibid.
65. U.S. Department of Homeland Security, Office of Inspector General, "TSA Can Improve Aviation Worker Vetting (Redacted)," OIG-15-98, June 2015, https://www.oig.dhs.gov/assets/Mgmt/2015/OIG_15-98_Jun15.pdf (accessed June 9, 2015).

66. Adam B. Lerner, "TSA, an 'Abominable Failure,'" *Politico*, June 2, 2015, <http://www.politico.com/story/2015/06/tsa-airport-security-failure-jeh-johnson-118557.html> (accessed June 9, 2015).
67. Transportation Security Administration, "Screening Partnership Program: Application Evaluation Process," https://www.tsa.gov/sites/default/files/publications/pdf/spp_application_evaluation_process_overview.pdf (accessed March 2, 2015).
68. Mike M. Ahlers and Jeanne Meserve, "TSA Shuts Door on Private Airport Screening Program," CNN, January 29, 2011, <http://www.cnn.com/2011/TRAVEL/01/29/tsa.private/> (accessed March 2, 2015), and news release, "House Leaders Put TSA on Notice for Implementing Reforms," Committee on Transportation and Infrastructure, U.S. House of Representatives, March 13, 2012, <http://archives.republicans.transportation.house.gov/News/PRArticle.aspx?NewsID=1551> (accessed March 2, 2015).
69. Transportation Security Administration, "Screening Partnership Program," January 2, 2015, <http://www.tsa.gov/stakeholders/screening-partnership-program> (accessed March 2, 2015).
70. Committee on Transportation and Infrastructure, U.S. House of Representatives, "TSA Ignores More Cost-Effective Screening Model," June 3, 2011, http://archives.republicans.transportation.house.gov/Media/file/112th/Aviation/2011-06-03-TSA_SPP_Report.pdf (accessed March 2, 2015).
71. Stephen M. Lord, Director, Homeland Security and Justice Issues, "Letter to Representative John L. Mica and Representative Daniel E. Lungren," March 4, 2011, <http://www.gao.gov/new.items/d11375r.pdf> (accessed March 2, 2015), and Robert Poole, "Modest Progress on Outsourced Checkpoint Screening," Reason Foundation *Airport Policy and Security News* No. 101, August 6, 2014, <http://reason.org/news/show/1013973.html#c> (accessed March 2, 2015).
72. Chris Edwards, "Privatizing the Transportation Security Administration," Cato Institute *Policy Analysis* No. 742, November 19, 2013, http://object.cato.org/sites/cato.org/files/pubs/pdf/pa742_web_1.pdf (accessed March 2, 2015).
73. Shirley Ybarra, "Overhauling U.S. Airport Security Screening," Reason Foundation *Policy Brief* No. 109, July 2013, http://reason.org/files/overhauling_airport_security.pdf (accessed March 2, 2015).
74. Poole, "Modest Progress on Outsourced Checkpoint Screening."
75. James Sherk, "Unionizing Airline Screeners Endangers National Security," Heritage Foundation *WebMemo* No. 3142, February 9, 2011, <http://www.heritage.org/research/reports/2011/02/unionizing-airline-screeners-endangers-national-security>.
76. Jessica Zuckerman, "Federal Flight Deck Officer Program: First Line of Deterrence, Last Line of Defense," Heritage Foundation *Issue Brief* No. 3544, March 20, 2012, <http://www.heritage.org/research/reports/2012/03/impact-of-cutting-the-budget-of-the-federal-flight-deck-officer-program>.
77. Transportation Security Administration, "Selection and Training," December 30, 2014, <http://www.tsa.gov/about-tsa/selection-and-training> (accessed May 5, 2015).
78. Zuckerman, "Federal Flight Deck Officer Program: First Line of Deterrence, Last Line of Defense"; Adam Minter, "Time to Ground Some of the Sky Police: Bloomberg Opinion," *Oregon Live*, March 16, 2015, http://www.oregonlive.com/opinion/index.ssf/2015/03/time_to_ground_the_sky_police.html (accessed July 20, 2015); and Air Line Pilots Association, International, "Securing Our Skies: Federal Flight Deck Officer Program," <http://www.alpa.org/advocacy/federal-flight-deck-officer-program> (accessed May 9, 2016).
79. Admiral Paul F. Zukunft, "Testimony on the Coast Guard Fiscal Year 2016 Budget Request," testimony before the Coast Guard and Maritime Transportation Subcommittee, Transportation and Infrastructure Committee, U.S. House of Representatives, February 25, 2015, <http://transportation.house.gov/uploadedfiles/2015-02-25-zukunft.pdf> (accessed May 14, 2015).
80. Ronald O'Rourke, "Coast Cutter Procurement: Background and Issues for Congress," Congressional Research Service *Report* R42567, April 15, 2016, <https://www.fas.org/sgp/crs/weapons/R42567.pdf> (accessed May 2, 2016).
81. Ibid.
82. Ibid.
83. Ibid.
84. Government Accountability Office, "Coast Guard: Better Logistics Planning Needed to Aid Operational Decisions Related to the Deployment of the National Security Cutter and Its Support Assets," GAO-09-497, July 2009, <http://www.gao.gov/assets/300/292572.pdf> (accessed May 2, 2016).
85. John C. Marcario, "UAS Priorities: Availability, Compatibility, Affordability Frame Coast Guard's Quest for Unmanned Aerial Capabilities," *Sea Power*, December 2011, <http://www.seapower-digital.com/seapower/201112?folio=46#pg48> (accessed May 2, 2016).
86. DHS Office of Inspector General, "U.S. Coast Guard's Acquisition of the Vertical-Takeoff-and-Landing Unmanned Aerial Vehicle," OIG-09-82, June 2009, http://www.oig.dhs.gov/assets/Mgmt/OIG_09-82_Jun09.pdf (accessed May 14, 2015).
87. Ibid., and John Egan, "The Unmanned Initiative: A Strategic Appraisal of Coast Guard Unmanned Aerial Systems," National Defense University, Joint Forces Staff College, Joint Advanced Warfighting School, June 10, 2011, <http://www.dtic.mil/dtic/tr/fulltext/u2/a545609.pdf> (accessed May 14, 2015).
88. Senate Report 113-077, "Department of Homeland Security Appropriations Bill, 2014," <http://thomas.loc.gov/cgi-bin/cpquery/T?&report=sr077&dbname=113&> (accessed May 14, 2015).

**CONGRESS MUST RE-SET DEPARTMENT OF HOMELAND SECURITY PRIORITIES:
AMERICAN LIVES DEPEND ON IT**

89. United States Coast Guard, "Fiscal Year 2017 Congressional Justification," https://www.uscg.mil/budget/docs/USCG_FY2017_Congressional_Justification.pdf (accessed May 13, 2016).
90. Hearing, "The President's Fiscal Year 2017 Budget Request for Coast Guard and Maritime Transportation Programs," Subcommittee on Coast Guard and Maritime Transportation, Transportation Committee, U.S. House of Representatives, 114th Cong., 2nd Sess., March 16, 2016, <http://transportation.house.gov/calendar/eventsingle.aspx?EventID=399880> (accessed May 2, 2016).
91. ABS Consulting, "United States Coast Guard High Latitude Region Mission Analysis Capstone Summary," June 2010, <http://assets.fiercemarkets.com/public/sites/govit/hlssummarycapstone.pdf> (accessed May 2, 2016).
92. Ronald O'Rourke, "Coast Guard Polar Icebreaker Modernization: Background and Issues for Congress," Congressional Research Service Report RL34391, April 22, 2015, <https://www.fas.org/sgp/crs/weapons/RL34391.pdf> (accessed May 2, 2016).
93. News release, "FACT SHEET: President Obama Announces New Investments to Enhance Safety and Security in the Changing Arctic," The White House, September 1, 2015, <https://www.whitehouse.gov/the-press-office/2015/09/01/fact-sheet-president-obama-announces-new-investments-enhance-safety-and> (accessed May 2, 2016).
94. Ibid.
95. Scott C. Truver, "Where Are the Icebreakers?!", *Breaking Defense*, January 11, 2016, <http://breakingdefense.com/2016/01/where-are-the-icebreakers/> (accessed May 2, 2016).
96. "Crashers Met Obama; Secret Service Apologizes," Associated Press, November 11, 2009, http://www.nbcnews.com/id/34173530/ns/politics-white_house/t/crashers-met-obama-secret-service-apologizes/#.VEqZCvnF98F (accessed October 24, 2014).
97. Carol D. Leonnig, "The Night Bullets Hit the White House—and the Secret Service Didn't Know," *The Washington Post*, September 28, 2014, http://www.washingtonpost.com/wp-srv/special/politics/white-house-shooting/?Post+generic=%3Ftid%3Dsm_twitter_washingtonpost (accessed October 24, 2014).
98. Ibid.
99. Michael Isikoff and Jim Miklaszewski, "NBC: Prostitute's \$50 Fee for Two Agents Triggered Secret Service Scandal," NBC News, April 17, 2012, http://usnews.nbcnews.com/_news/2012/04/17/11251326-nbc-prostitutes-50-fee-for-two-agents-triggered-secret-service-scandal?lite (accessed October 24, 2014).
100. "2 Secret Service Supervisors Under Investigation in Misconduct Probe," CNN, November 14, 2013, <http://www.cnn.com/2013/11/14/politics/secret-service-misconduct/> (accessed October 24, 2014), and Sebastian Payne, "A Shortlist of Recent Secret Service Scandals," *The Washington Post*, October 1, 2014, <http://www.washingtonpost.com/blogs/post-politics/wp/2014/10/01/a-shortlist-of-recent-secret-service-scandals/> (accessed October 30, 2014).
101. Carol D. Leonnig and David Nakamura, "Secret Service Agents Sent Home from Netherlands Were Warned to Avoid Trouble," *The Washington Post*, March 26, 2014, http://www.washingtonpost.com/politics/secret-service-agents-on-obama-detail-sent-home-from-netherlands-after-night-of-drinking/2014/03/26/86d1a8a6-b4e6-11e3-8020-b2d790b3c9e1_story.html (accessed October 24, 2014).
102. Carol D. Leonnig, "Armed Contractor with Criminal Record Was on Elevator with Obama in Atlanta," *The Washington Post*, September 30, 2014, http://www.washingtonpost.com/politics/armed-former-convict-was-on-elevator-with-obama-in-atlanta/2014/09/30/76d7da24-48e3-11e4-891d-713f052086a0_story.html (accessed October 29, 2014).
103. Carol D. Leonnig, "White House Fence-Jumper Made It Far Deeper into Building than Previously Known," *The Washington Post*, September 29, 2014, http://www.washingtonpost.com/politics/white-house-fence-jumper-made-it-far-deeper-into-building-than-previously-known/2014/09/29/02efd53e-47ea-11e4-a046-120a8a855cca_story.html (accessed October 29, 2014).
104. Carol D. Leonnig and David Nakamura, "Aides Knew of Possible White House Link to Cartagena, Colombia, Prostitution Scandal," *The Washington Post*, October 8, 2014, http://www.washingtonpost.com/politics/aides-despite-denials-knew-of-white-house-tie-to-cartagena-prostitution-scandal/2014/10/08/5b98dc90-4e7e-11e4-aa5e-7153e466a02d_story.html (accessed May 14, 2015).
105. Carol D. Leonnig, "Secret Service Agents Investigated after Car Hits White House Barricade," *The Washington Post*, March 11, 2015, http://www.washingtonpost.com/politics/secret-service-agents-investigated-for-late-night-car-accident-at-white-house/2015/03/11/9c853906-c7ff-11e4-a199-6cb5e63819d2_story.html (accessed July 23, 2015).
106. John Roth, "U.S. Secret Service: Accountability for March 4, 2015," statement before the Committee on Oversight and Government Reform, U.S. House of Representatives, May 14, 2015, https://www.oig.dhs.gov/assets/TM/2015/OIGtm_JR_051415.pdf (accessed May 14, 2015).
107. Carol D. Leonnig, "Secret Service Agent Retiring Amid Probe into Conduct at White House," *The Washington Post*, May 13, 2015, http://www.washingtonpost.com/politics/secret-service-agent-retiring-amid-probe-into-conduct-at-white-house/2015/05/13/86de428c-f806-11e4-a13c-193b1241d51a_story.html (accessed May 14, 2015).
108. Carol D. Leonnig and Keith L. Alexander, "Secret Service Manager Put on Leave During Probe of Alleged Assault," *The Washington Post*, April 8, 2015, http://www.washingtonpost.com/politics/secret-service-manager-put-on-leave-after-alleged-assault-at-headquarters/2015/04/08/cb31c412-ddf9-11e4-a500-1c5bb1d8ff6a_story.html (accessed July 21, 2015).

109. ABC News, "Secret Service Officer Put on Leave After Arrest," April 10, 2015, <http://abcnews.go.com/Politics/wireStory/secret-service-officer-put-leave-arrest-30231324> (accessed May 5, 2015).
110. Office of the Inspector General, Department of Homeland Security, "Memorandum," September 25, 2015, https://www.oig.dhs.gov/assets/Mga/OIG_mga-092515.pdf (accessed April 13, 2016).
111. Best Places to Work in the Federal Government, "Secret Service (DHS)," 2015, <http://bestplacestowork.org/BPTW/rankings/detail/HS14> (accessed March 10, 2016).
112. Joseph W. Hagin et al., "United States Secret Service Protective Mission Panel (USSSPMP)," letter to Jeh Johnson, December 15, 2014, http://www.dhs.gov/sites/default/files/publications/14_1218_ussp_pmp.pdf (accessed July 21, 2015).
113. Ibid.
114. Arlette Saenz, "Metal Spikes Installed on White House Fence in Latest Security Renovation," ABC News, July 1, 2015, <http://abcnews.go.com/Politics/metal-spikes-installed-white-house-fence-latest-security/story?id=32163777> (accessed July 30, 2015).
115. Ibid.
116. Ibid.
117. U.S. Department of Defense, "The Department of Defense Cyber Strategy," April 2015, http://www.defense.gov/home/features/2015/0415_cyberstrategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (accessed September 2, 2015).
118. "U.S. Government Ranks Last Among Major Industries in Cybersecurity," SecurityScorecard, April 14, 2016, <http://www.prnewswire.com/news-releases/us-government-ranks-last-among-major-industries-in-cybersecurity-300251604.html> (accessed April 29, 2016).
119. Department of Homeland Security, "About the National Cybersecurity and Communications Integration Center," April 27, 2015, <http://www.dhs.gov/about-national-cybersecurity-communications-integration-center> (accessed September 2, 2015).
120. Evan McDermott and David Inserra, "Why Cybersecurity Information Sharing Is a Positive Step for Online Security," The Daily Signal, January 25, 2016, <http://dailysignal.com/2016/01/25/why-cybersecurity-information-sharing-is-a-positive-step-for-online-security/>.
121. Margaret Rouse, "Trusted Internet Connections (TIC)," What Is.com, April 2010, <http://whatis.techtarget.com/definition/Trusted-Internet-Connections-TIC> (accessed July 22, 2015), and Eric Chabrow, "What's Happening with the Trusted Internet Connection?" GovInfoSecurity, March 1, 2010, <http://www.govinfosecurity.com/interviews.php?interviewID=451> (accessed August 26, 2015).
122. U.S. Department of Homeland Security, "EINSTEIN 3 Accelerated," April 17, 2015, <http://www.dhs.gov/publication/einstein-3-accelerated> (accessed July 22, 2015).
123. U.S. Government Accountability Office, "Information Security: DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System," GAO-16-294, January 2016, <http://www.gao.gov/assets/680/674829.pdf> (accessed April 13, 2016).
124. Ibid., and U.S. Computer Emergency Readiness Team, "Continuous Diagnostics and Mitigation (CDM)," 2015, <https://www.us-cert.gov/cdm> (accessed July 22, 2015).
125. Ibid.
126. U.S. Department of Homeland Security, "Enhanced Cybersecurity Services," May 27, 2015, <http://www.dhs.gov/enhanced-cybersecurity-services> (accessed July 22, 2015).
127. MITRE, "STIX-Structured Threat Information eXpression," March 25, 2015, <http://stix.mitre.org/> (accessed July 22, 2015).
128. MITRE, "TAXII-Trusted Automated eXchange of Indicator Information," April 14, 2015, <http://taxii.mitre.org/> (accessed July 22, 2015).
129. U.S. Department of Homeland Security, "About the Critical Infrastructure Cyber Community C³ Voluntary Program," June 17, 2015, <http://www.dhs.gov/about-critical-infrastructure-cyber-community-c%C2%B3-voluntary-program> (accessed July 22, 2015).
130. Eric A. Fischer et al., "The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress," Congressional Research Service Report R42984, December 15, 2014, <http://blogs.fas.org/sgp/crs/misc/R42984.pdf> (accessed July 22, 2015).
131. Paul Rosenzweig and David Inserra, "Obama's Cybersecurity Executive Order Falls Short," Heritage Foundation *Issue Brief* No. 3852, February 14, 2015, <http://www.heritage.org/research/reports/2013/02/obama-s-cybersecurity-executive-order-falls-short>.
132. Department of Homeland Security, "DHS' Efforts to Coordinate the Activities of Federal Cyber Operations Centers," OIG-14-02, October 2013, http://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-02_Oct13.pdf (accessed July 22, 2015).
133. Jerry Markon, Ellen Nakashima, and Alice Crites, "Top-Level Turnover Makes it Harder for DHS to Stay on Top of Evolving Threats," *The Washington Post*, September 21, 2014, http://www.washingtonpost.com/politics/top-level-turnover-makes-it-harder-for-dhs-to-stay-on-top-of-evolving-threats/2014/09/21/ca7919a6-39d7-11e4-9c9f-ebb47272e40e_story.html?tid=HP_lede (accessed July 22, 2015), and Sean Lyngaas, "Can DHS Get It Together?" FCW, October 31, 2014, <http://fcw.com/Articles/2014/10/31/Cybersecurity-Can-DHS-get-it-together.aspx?Page=2> (accessed July 22, 2015).

**CONGRESS MUST RE-SET DEPARTMENT OF HOMELAND SECURITY PRIORITIES:
AMERICAN LIVES DEPEND ON IT**

134. "Obama Signs Five Cybersecurity Measures into Law," Homeland Security News Wire, December 23, 2014, <http://www.homelandsecuritynewswire.com/dr20141223-obama-signs-five-cybersecurity-measures-into-law> (accessed July 22, 2015).
135. Richard Bejtlich, "What Are the Prospects for the Cyber Threat Intelligence Integration Center?" Brookings Institution, February 19, 2015, <http://www.brookings.edu/blogs/techtank/posts/2015/02/19-cyber-security-center-bejtlich> (accessed July 22, 2015).
136. Government Accountability Office, "Agencies Need to Improve Cyber Incident Response Practices," GAO-14-354, May 30, 2014, <http://www.gao.gov/products/GAO-14-354> (accessed July 22, 2015).
137. Phyllis Schneck, "DHS Cyber Chief Emphasizes Resiliency, Building Trust," *Federal Times*, September 26, 2014, <http://www.federaltimes.com/article/20140926/DHS02/309260015/DHS-cyber-chief-emphasizes-resiliency-building-trust> (accessed July 22, 2015).
138. Department of Homeland Security Office of Inspector General, "Implementation Status of the Enhanced Cybersecurity Services Program," OIG-14-119, July 2014, http://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-119_Jul14.pdf (accessed July 22, 2015).
139. Government Accountability Office, "DHS and GSA Should Address Cyber Risk to Building and Access Control Systems," GAO-15-6, January 12, 2015, <http://www.gao.gov/products/GAO-15-6> (accessed July 22, 2015); Government Accountability Office, "Cybersecurity: Actions Needed to Address Challenges Facing Federal Systems," GAO-15-573T, April 22, 2015, <http://www.gao.gov/products/GAO-15-573T> (accessed July 22, 2015); and Government Accountability Office, "Information Security: Agencies Need to Improve Cyber Incident Response Practices," GAO-14-354, April 30, 2014, <http://www.gao.gov/products/GAO-14-354> (accessed July 22, 2015).
140. Amber Corrin, "Does Cyber Breach Illuminate a \$3B DHS Failure?" C4ISR & Networks, June 5, 2015, <http://www.c4isrnet.com/story/military-tech/cyber/2015/06/05/opm-breach-einstein-dhs/28556635/> (accessed June 11, 2015).
141. Department of Homeland Security, "National Coordinating Center Communications," September 16, 2014, <http://www.dhs.gov/national-coordinating-center-communications> (accessed July 22, 2015).
142. Department of Homeland Security, "About the Office Emergency Communications," December 8, 2014, <http://www.dhs.gov/about-office-emergency-communications> (accessed July 22, 2015).
143. U.S. Department of Homeland Security, Office of Inspector General, "DHS' Oversight of Interoperable Communications," OIG-13-06, November 2012, https://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-06_Nov12.pdf (accessed June 9, 2015).
144. U.S. Department of Homeland Security, Office of Inspector General, "Corrective Actions Still Needed to Achieve Interoperable Communications," OIG-15-97-VR, May 2015, https://www.oig.dhs.gov/assets/GrantReports/2015/OIG_15-97-VR_May15.pdf (accessed June 9, 2015).
145. Department of Homeland Security, "National Infrastructure Protection Plan," June 16, 2015, <http://www.dhs.gov/national-infrastructure-protection-plan> (accessed July 22, 2015).
146. Department of Homeland Security, "Sector Outreach and Programs Division," April 24, 2014, <http://www.dhs.gov/sopd> (accessed July 22, 2015).
147. Department of Homeland Security, "National Infrastructure Protection Plan."
148. Department of Homeland Security, "Sector Outreach and Programs Division."
149. Government Accountability Office, "Critical Infrastructure Protection: DHS Efforts to Assess Chemical Security Risk and Gather Feedback on Facility Outreach Can Be Strengthened," GAO-13-353, April 2013, <http://www.gao.gov/assets/660/653601.pdf> (accessed July 22, 2015).
150. Ibid.
151. Ibid.
152. Jessica Zuckerman and David Inserra, "Chemical Security: Risk-Based Solutions Key to Fixing Flaws," Heritage Foundation *Issue Brief* No. 3901, April 9, 2013, <http://www.heritage.org/research/reports/2013/04/chemical-security-risk-based-solutions-key-to-fixing-flaws>.
153. Ibid.
154. The personnel surety standard is designed to ensure that workers and certain visitors are who they say they are, and that they have undergone a background check for criminal and terrorist ties or history.
155. H.R. 4007, Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014, 113th Congress, 2nd Sess., <https://www.congress.gov/bill/113th-congress/house-bill/4007/text> (accessed July 22, 2015).
156. Stephen L. Caldwell, "Critical Infrastructure Protection: Observations on DHS Efforts to Implement and Manage Its Chemical Security Program," GAO-14-608T, May 14, 2014, <http://www.gao.gov/assets/670/663170.pdf> (accessed July 22, 2015).
157. Government Accountability Office, "Budget Issues: Better Fee Design Would Improve Federal Protective Service's and Federal Agencies' Planning and Budgeting for Security," GAO-11-492, May 2011, <http://www.gao.gov/assets/320/318668.pdf> (accessed July 22, 2015).
158. Hannah Hess, "Advocates Still Hope for Federal Protective Service Overhaul," *Roll Call*, January 6, 2014, http://www.rollcall.com/news/advocates_still_hope_for_federal_protective_service_overhaul-229927-1.html (accessed September 2, 2015).
159. Government Accountability Office, Recommendations Database, Keyword search "FPS," http://www.gao.gov/recommendations/search?searched=1&hide_order_by_block=1&expand=&openrecs=&q=FPS&field=recommendation_text_s (accessed April 18, 2016).

160. Mark Goldstein, "Federal Protective Service: Protecting Federal Facilities Remains a Challenge," GAO-14-623T, May 21, 2014, <http://www.gao.gov/assets/670/663347.pdf> (accessed July 22, 2015).
161. Ibid.
162. Government Accountability Office, "Federal Protective Service: More Effective Management Needed in Delegating Security Authority to Agencies," GAO-15-271, March 31, 2015, <http://www.gao.gov/products/GAO-15-27> (accessed July 22, 2015).
163. Jack Moore, "Lawmakers Worried DHS Losing Faith in Federal Protective Service," Federal News Radio, May 21, 2014, <http://federalnewsradio.com/congress/2014/05/lawmakers-worried-dhs-losing-faith-in-federal-protective-service/> (accessed July 22, 2015).
164. IT Dashboard, "NPPD-OBIM-Automated Biometric Identification System (IDENT)," FY 2016 Edition, <https://itdashboard.gov/investment?buscid=151> (accessed July 23, 2015).
165. FBI, "Integrated Automated Fingerprint Identification System (IAFIS)," 2015, http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis (accessed May 5, 2015).
166. IT Dashboard, "Evaluation History: NPPD-OBIM-Automated Biometric Identification System (IDENT)," FY 2016 Edition, <https://itdashboard.gov/investment/evaluation-history/151> (accessed July 23, 2015).
167. IT Dashboard, "NPPD-OBIM-Automated Biometric Identification System (IDENT)."
168. U.S. Department of Homeland Security, TSA Office of Intelligence and Analysis, "Privacy Impact Assessment," March 2014, <https://www.dhs.gov/sites/default/files/publications/privacy-pia-tsa-oia-technology-infrastructure-modernization-program-03-26-14.pdf> (accessed April 13, 2016).
169. U.S. Department of Homeland Security, Citizenship and Immigration Services, "Privacy Impact Assessment," March 8, 2016, <https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis-pcqs-march2016.pdf> (accessed April 13, 2016).
170. Government Accountability Office, "Budget Issues: Better Fee Design Would Improve Federal Protective Service's and Federal Agencies' Planning and Budgeting for Security," GAO-11-492, May 20, 2011, <http://www.gao.gov/products/GAO-11-492> (accessed July 23, 2015).
171. FEMA has large sums rescinded in the past few years that lowers the effective money that FEMA has available. In 2015, \$400 million was rescinded while in 2016 about \$1 billion was rescinded, leaving FEMA with about \$15.5 billion for each year. The President has requested a \$16.9 billion budget for FY 2017 but also includes a \$400 million rescission for a total of around \$16.5 billion.
172. David Inserra, "FEMA Reform Needed: Congress Must Act," Heritage Foundation *Issue Brief* No. 4342, February 4, 2015, <http://www.heritage.org/research/reports/2015/02/fema-reform-needed-congress-must-act>.
173. Ellen Prichard and David Inserra, "Where Does Your State Rank in Disaster Preparedness?" The Daily Signal, December 12, 2014, <http://dailysignal.com/2014/12/12/state-rank-disaster-preparedness/>.
174. 42 U.S. Code § 5170.
175. Ibid.
176. News release, "Dr. Coburn Releases Report on the Fleecing of Taxpayers through Disaster Declarations," U.S. Senate Homeland Security and Governmental Affairs Committee, December 31, 2014, <http://www.hsgac.senate.gov/media/minority-media/dr-coburn-releases-report-on-the-fleecing-of-taxpayers-through-disaster-declarations> (accessed January 29, 2015).
177. Federal Emergency Management Agency, "Disaster Declarations for 2014," https://www.fema.gov/disasters/grid/year/2014?field_disaster_type_term_tid_1=All (accessed May 5, 2015). Data on emergency declarations and fire-management-assistance declarations is less available, but doubtless some fires and emergencies would not reach the higher threshold.
178. Federal Emergency Management Agency, "Preparedness (Non-Disaster) Grants," August 6, 2014, <https://www.fema.gov/preparedness-non-disaster-grants> (accessed January 29, 2015).
179. David Perera, "House and Senate Appropriators Reject National Preparedness Grant Program Proposal," Fierce Homeland Security, May 16, 2012, <http://www.fiercehomelandsecurity.com/story/house-and-senate-appropriations-reject-national-preparedness-grant-program/2012-05-16> (accessed January 29, 2015).
180. Jena Baker McNeill and Matt A. Mayer, "Homeland Security Grants Should Not Become Another Federal Entitlement Program," Heritage Foundation *WebMemo* No. 3151, February 14, 2011, <http://www.heritage.org/research/reports/2011/02/homeland-security-grants-should-not-become-another-federal-entitlement-program>.
181. "Sen. Coburn Questions Homeland Security Spending," Fox Business, December 5, 2012, video, <http://video.foxbusiness.com/v/2014282289001/sen-coburn-questions-homeland-security-spending/?#sp=show-clips> (accessed January 29, 2015).
182. David B. Muhlhause, "Fire Grants: Do Not Reauthorize an Ineffective Program," Heritage Foundation *Issue Brief* No. 3505, February 15, 2012, <http://www.heritage.org/research/reports/2012/02/fire-grants-do-not-reauthorize-an-ineffective-program>.
183. Government Accountability Office, "High-Risk Series: An Update—National Flood Insurance Program" GAO-15-290, February 11, 2015, http://www.gao.gov/highrisk/national_flood_insurance/why_did_study#t=0 (accessed July 23, 2015).

**CONGRESS MUST RE-SET DEPARTMENT OF HOMELAND SECURITY PRIORITIES:
AMERICAN LIVES DEPEND ON IT**

184. Homeowner Flood Insurance Affordability Act of 2014, H.R. 3370, 113th Cong., 2nd Sess. (2014), <https://www.congress.gov/bill/113th-congress/house-bill/3370> (accessed July 23, 2014).
185. Deborah Barfield Berry, "Flood Insurance Bill Clears Congress," *USA Today*, March 13, 2014, <http://www.usatoday.com/story/news/nation/2014/03/13/flood-insurance-bill-clears-congress/6384095/> (accessed July 23, 2015).
186. Government Accountability Office, "Flood Insurance: Forgone Premiums Cannot Be Measured and FEMA Should Validate and Monitor Data System Changes," GAO-15-111, December 11, 2014, <http://www.gao.gov/products/GAO-15-111> (accessed July 23, 2015).
187. Government Accountability Office, "High-Risk Series: An Update National Flood Insurance Program."
188. Government Accountability Office, "Overview of GAO's Past Work on the National Flood Insurance Program," April 9, 2014, <http://www.gao.gov/assets/670/662438.pdf> (accessed July 23, 2015).
189. Warren Mass, "Illegal Immigrants Eligible for Earned Income Tax Credit, Other Benefits," *New American*, February 18, 2015, <http://www.thenewamerican.com/usnews/immigration/item/20149-illegal-immigrants-eligible-for-earned-income-tax-credit-other-benefits> (accessed July 23, 2015), and National Immigration Law Center, "DAPA & Expanded DACA," March 2, 2015, <http://www.nilc.org/dapa&daca.html> (accessed July 23, 2015).
190. *Texas v. United States*, No. B-14-254, 2015 WL 648579 (S.D. Tex. Feb. 16, 2015).
191. Caroline May, "Immigration Officers' Union: End Political Corruption in Immigration Before Amnesty," *The Daily Caller*, October 10, 2013, <http://dailycaller.com/2013/10/10/immigration-officers-union-end-political-corruption-in-immigration-before-amnesty/#ixzz2hL28BMZS> (accessed April 18, 2016).
192. Ibid.
193. U.S. Department of Homeland Security, Office of Inspector General, "The Effects of USCIS Adjudication Procedures and Policies on Fraud Detection by Immigration Service Officers," OIG-12-24, January 2012, http://www.oig.dhs.gov/assets/Mgmt/OIG_12-24_Jan12.pdf (accessed April 18, 2016).
194. "Documents Reveal DHS Abandoned Illegal Alien Background Checks to Meet Amnesty Requests Following Obama's DACA," Judicial Watch, June 11, 2013, <http://www.judicialwatch.org/press-room/press-releases/homeland-security-documents-reveal-dhs-abandoned-required-illegal-alien-background-checks-to-meet-flood-of-amnesty-requests-following-obamas-deferred-action-for-childhood-arrivals-directive/> (accessed April 18, 2016).
195. News release, "IG Concludes Investigation of Employee Complaints Regarding Management of USCIS' EB-5 Program," Department of Homeland Security Office of Inspector General, March 24, 2014, http://www.oig.dhs.gov/assets/pr/2015/oigpr_032415.pdf (accessed July 23, 2015).
196. Department of Homeland Security Office of Inspector General, "Investigation into Employee Complaints about Management of U.S. Citizenship and Immigration Services' EB-5 Program," memorandum to Jeh Johnson, March 24, 2015, http://www.oig.dhs.gov/assets/Mga/OIG_mga-032415.pdf (accessed July 23, 2015). In its investigation, the Inspector General found that "the number and variety of witnesses is highly unusual. It is also unusual that a significant percentage of witnesses...would talk to us only after being assured that their identities would remain confidential.... That so many individuals were willing to step forward and tell us what happened is evidence of deep resentment about Mr. Mayorkas' actions related to the EB-5 program.... Their allegations were unequivocal: Mr. Mayorkas gave special access and treatment to certain individuals and parties.... Employees felt uncomfortable and pressured to comply with managers' instructions that appeared to have come from Mr. Mayorkas.... Again, these comments were not from one or even a couple of disgruntled employees with axes to grind; rather these were individuals throughout the ranks of USCIS, in different locations, engaged in different functions, with different levels of experience."
197. News release, "Statement by Secretary Jeh C. Johnson about the DHS Inspector General's Report Concerning Deputy Secretary Mayorkas," Department of Homeland Security, March 24, 2015, <http://www.dhs.gov/news/2015/03/24/statement-secretary-jeh-c-johnson-about-dhs-inspector-generals-report-concerning-0> (accessed July 23, 2015).
198. Josh Gerstein, "Report Cites Favoritism for Terry McAuliffe and Brother of Hillary Clinton," *Politico*, March 24, 2015, http://www.politico.com/story/2015/03/report-cites-favoritism-for-terry-mcauliffe-and-brother-of-hillary-clinton-116370.html?hp=t2_r (accessed July 23, 2015).
199. Jack Moore, "Background Investigation Fraud Case Against USIS Moved to DC Court," Federal News Radio, May 7, 2014, <http://www.federalnewsradio.com/520/3618119/Background-investigation-fraud-case-against-USIS-moved-to-DC-court> (accessed August 28, 2014).
200. Hans A. von Spakovsky, "Arizona v. United States: What the States Can Do to Enforce Immigration Laws," Heritage Foundation *Issue Brief* No. 3649, June 27, 2012, <http://www.heritage.org/research/reports/2012/06/supreme-court-decision-on-arizona-immigration-law>.
201. Charles Stimson, "States Get a 'License' to Enforce Immigration Laws," Heritage Foundation *WebMemo* No. 3342, August 22, 2011, <http://www.heritage.org/research/reports/2011/08/ruling-on-states-immigration-law-enforcement-and-verify-use>.
202. U.S. Citizenship and Immigration Services, "E-Verify Program Statistics: Performance," January 21, 2014, <http://www.uscis.gov/e-verify/about-program/performance> (accessed July 30, 2014), and Westat, "Evaluation of the Accuracy of E-Verify Findings: Report Submitted to U.S. Department of Homeland Security," July 2012, p. x, http://www.uscis.gov/sites/default/files/USCIS/Verification/E-Verify/E-Verify_Native_Documents/EVerify%20Studies/Evaluation%20of%20the%20Accuracy%20of%20EVerify%20Findings.pdf (accessed July 30, 2014).

-
203. U.S. Citizenship and Immigration Services, "E-Verify Program Statistics."
 204. Westat, "Evaluation of the Accuracy of E-Verify Findings."
 205. U.S. Citizenship and Immigration Services, "Self Check Background," September 18, 2013, <http://www.uscis.gov/self-check/self-check-background> (accessed August 28, 2014).
 206. Marc R. Rosenblum, "E-Verify: Strengths, Weaknesses, and Proposals for Reform," Migration Policy Institute, February 2011, <http://www.migrationpolicy.org/research/e-verify-strengths-weaknesses-and-proposals-reform> (accessed July 30, 2015), and Westat, "Findings of the E-Verify Program Evaluation," December 2009, http://www.uscis.gov/sites/default/files/USCIS/E-Verify/E-Verify/Final%20E-Verify%20Report%2012-16-09_2.pdf (accessed July 30, 2015).
 207. "Paris Attacks: Who Were the Attackers?" BBC, March 18, 2016, <http://www.bbc.com/news/world-europe-34832512> (accessed April 13, 2016).
 208. David Inserra, "2 Refugees Charged With Supporting Terrorism. Is Obama Doing Enough to Keep America Safe?" Daily Signal, January 12, 2016, <http://dailysignal.com/2016/01/12/two-charged-with-supporting-terrorism-administration-must-prove-it-is-up-to-the-task-on-refugees/>, and Riley Walters and Alexis Mrachek, "Already, 3 Islamist Terror Plot Attempts in US This Year," The Daily Signal, February 2, 2016, <http://dailysignal.com/2016/02/02/already-3-islamist-terror-plots-attempts-in-us-this-year/>.
 209. Inserra, "2 Refugees Charged With Supporting Terrorism."
 210. Chuck Ross, "FBI Director Admits US Can't Vet All Syrian Refugees for Terror Ties [VIDEO]," *The Daily Caller*, October 21, 2015, <http://dailycaller.com/2015/10/21/fbi-director-admits-us-cant-vet-all-syrian-refugees-for-terror-ties-video/> (accessed April 29, 2016).
 211. Aliya Sternstein, "DHS to Recompete Online Immigration Program in 'Crisis,'" Nextgov, December 13, 2012, <http://www.nextgov.com/defense/2012/12/dhs-recompete-online-immigration-program-crisis/60144/> (accessed July 30, 2015).
 212. U.S. Citizenship and Immigration Services, "USCIS Electronic Immigration System (ELIS)," July 15, 2015, <http://www.uscis.gov/uscis-elis> (accessed July 23, 2015).
 213. Aliya Sternstein, "DHS Takes a Second Stab at Automating Immigration Casework," Nextgov, March 28, 2014, <http://www.nextgov.com/cio-briefing/2014/03/dhs-takes-second-stab-automating-immigration-casework/81535/> (accessed July 30, 2015).
 214. U.S. Department of Homeland Security, Office of Inspector General, "USCIS Automation of Immigration Benefits Processing Remains Ineffective," March 9, 2016, <https://www.oig.dhs.gov/assets/Mgmt/2016/OIG-16-48-Mar16.pdf> (accessed April 14, 2016).
 215. Department of Homeland Security, Chief Information Officer, "IT Dashboard: ELIS Evaluation History," August 4, 2014, <https://www.itdashboard.gov/print/investment/evaluation-history/319> (accessed July 30, 2015).
 216. Government Accountability Office, "Immigration Benefits: Consistent Adherence to DHS's Acquisition Policy Could Help Improve Transformation Program Outcomes," GAO-12-66, November 2011, <http://www.gao.gov/assets/590/586460.pdf> (accessed July 30, 2015).
 217. Louis D. Crocetti Jr., "Asylum Fraud: Abusing America's Compassion?" testimony before the Subcommittee on Immigration and Border Security, Judiciary Committee, U.S. House of Representatives, February 11, 2014, http://judiciary.house.gov/_cache/files/aea7ea4f-7974-4181-9798-7654f3fe901a/crocetti-house-judiciary-asylum-fraud-testimony-final-2-7-14.pdf (accessed July 30, 2014).
 218. Ibid.
 219. U.S. Government Accountability Office, "Asylum: Additional Actions Needed to Assess and Address Fraud Risks," GAO-16-50, December 2, 2015, <http://www.gao.gov/assets/680/673941.pdf> (accessed April 14, 2016).
 220. Ibid.
 221. Dagmar R. Myslinska, "Your Rights After a Grant of Asylum," Nolo, <http://www.nolo.com/legal-encyclopedia/your-rights-after-grant-asylum.html> (accessed July 30, 2014), and U.S. Citizenship and Immigration Services, "Benefits and Responsibilities of Asylees," April 1, 2011, <http://www.uscis.gov/humanitarian/refugees-asylum/asylum/benefits-and-responsibilities-asylees> (accessed July 30, 2015).
 222. Department of Homeland Security, U.S. Citizenship and Immigration Service, "Public Charge," September 3, 2009, <http://www.uscis.gov/green-card/green-card-processes-and-procedures/public-charge> (accessed August 28, 2014).
 223. Eyder Perlata, "Immigration Officers' Union Will Oppose Senate Bill," NPR, May 20, 2013, <http://www.npr.org/sections/thetwo-way/2013/05/20/185520730/immigration-officers-union-will-oppose-senate-bill> (accessed July 30, 2015).
 224. White House Task Force on New Americans, "Strengthening Communities by Welcoming All Residents: A Federal Strategic Action Plan on Immigrant & Refugee Integration," The White House, April 2015, pp. 13, 16, 17, 24-30, 37, and 40, https://www.whitehouse.gov/sites/default/files/docs/final_tf_newamericans_report_4-14-15_clean.pdf (accessed April 22, 2015).
 225. Mike Gonzalez, "The Task Force on New Americans: Congress Must Examine the Federal Strategic Action Plan," Heritage Foundation *Issue Brief* No. 4394, April 28, 2015, <http://www.heritage.org/research/reports/2015/04/the-task-force-on-new-americans-congress-must-examine-the-federal-strategic-action-plan>.
 226. Ibid.
 227. John Fonte, *Sovereignty or Submission: Will Americans Rule Themselves or Be Ruled by Others?* (New York: Encounter Books, 2011).
-

**CONGRESS MUST RE-SET DEPARTMENT OF HOMELAND SECURITY PRIORITIES:
AMERICAN LIVES DEPEND ON IT**

228. Brian A. Reaves, "Census of State and Local Law Enforcement Agencies, 2008," U.S. Department of Justice, NCJ 233982, July 2011, <http://www.bjs.gov/content/pub/pdf/cslea08.pdf> (accessed July 23, 2015).
229. Federal Law Enforcement Training Centers, 2015, <https://www.fletc.gov/> (accessed July 23, 2015).
230. Department of Homeland Security, *Budget-in-Brief, Fiscal Year 2017*, <https://www.dhs.gov/sites/default/files/publications/FY2017BIB.pdf> (accessed April 14, 2016).
231. U.S. Department of Homeland Security, Office of the Inspector General, "DHS' Oversight of Its Workforce Training Needs Improvement," January 20, 2016, <https://www.oig.dhs.gov/assets/Mgmt/2016/OIG-16-19-Jan16.pdf> (accessed April 14, 2016).
232. Ibid.
233. Senator Tom Coburn, "A Review of the Department of Homeland Security's Missions and Performance," Committee on Homeland Security and Governmental Affairs, U.S. Senate, January 2015, p. 148.
234. Dana A. Shea, "The DHS S&T Directorate: Selected Issues for Congress," Congressional Research Service Report R43064, April 14, 2014, <http://www.fas.org/sgp/crs/homesecc/R43064.pdf> (accessed July 23, 2015).
235. Department of Homeland Security, "Science and Technology: About the First Responders Group," <http://www.dhs.gov/science-and-technology/about-first-responders> (accessed July 23, 2015).
236. Department of Homeland Security, "About Research and Development Partnerships," May 5, 2015, <http://www.dhs.gov/science-and-technology/about-research-and-development-partnerships> (accessed July 23, 2015).
237. Department of Homeland Security, "Science and Technology: About the Homeland Security Advanced Research Projects Agency," <http://www.dhs.gov/science-and-technology/about-hsarpa> (accessed July 23, 2015).
238. Department of Homeland Security, "Science and Technology: Capability Development Support," <http://www.dhs.gov/science-and-technology/about-cds> (accessed July 23, 2015).
239. Shea, "The DHS S&T Directorate: Selected Issues for Congress."
240. Coburn, "A Review of the Department of Homeland Security's Missions and Performance," pp. 137-139.
241. Ibid., p. 137.
242. "Strategy and Mission of the DHS Science and Technology Directorate," joint hearing before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, Committee on Homeland Security, U.S. House of Representatives, and Subcommittee on Research and Technology, Committee on Science, Space, and Technology, U.S. House of Representatives, 113th Cong., 2nd Sess., September 9, 2014, p. 22, <http://www.gpo.gov/fdsys/pkg/CHRG-113hrg92900/pdf/CHRG-113hrg92900.pdf> (accessed July 23, 2015).
243. Jared Serbu, "DHS S&T Chief Plans for More Relevant Research, Better Employee Morale," Federal News Radio, September 12, 2014, <http://www.federalnewsradio.com/480/3700433/DHS-ST-chief-plans-for-more-relevant-research-better-employee-morale> (accessed July 23, 2015).
244. Government Accountability Office, "Department of Homeland Security: Continued Actions Needed to Strengthen Oversight and Coordination of Research and Development," GAO-14-813T, July 31, 2014, <http://www.gao.gov/assets/670/665128.pdf> (accessed April 18, 2016).
245. Ibid., and Office of Management and Budget, OMB Circular A-11, Section 84, 2015, https://www.whitehouse.gov/sites/default/files/omb/assets/a11_current_year/s84.pdf (accessed August 26, 2015).
246. "Strategy and Mission of the DHS Science and Technology Directorate," joint hearing.
247. Ibid.
248. Government Accountability Office, "Department of Homeland Security: Oversight and Coordination of Research and Development Should Be Strengthened," GAO-12-837, September 12, 2012, <http://www.gao.gov/products/GAO-12-837> (accessed July 23, 2015).
249. Department of Homeland Security, "SAFETY Act," <https://www.safetyact.gov/pages/homepages/Home.do> (accessed May 5, 2015).
250. Ibid.
251. Paul Rosenzweig, Jena Baker McNeill, and James Jay Carafano, "Using the SAFETY Act to Build a Stronger U.S.-Israeli Terrorism-Fighting Partnership," Heritage Foundation *WebMemo* No. 3077, December 8, 2010, <http://www.heritage.org/research/reports/2010/12/using-the-safety-act-to-build-a-stronger-us-israeli-terrorism-fighting-partnership>.
252. Best Places to Work in the Federal Government, "Office of the Under Secretary for Science and Technology (DHS)," 2015, <http://bestplacestowork.org/BPTW/rankings/detail/HSFA> (accessed April 29, 2016).
253. News release, "DHS Announces Expansion of the Securing the Cities Program to the National Capital Region," Department of Homeland Security, September 2, 2014, <http://www.dhs.gov/news/2014/09/02/dhs-announces-expansion-securing-cities-program-national-capital-region> (accessed July 23, 2015), and Department of Homeland Security, "DHS Supports Exercise of Securing the Cities Program Designed to Detect Radiological and Nuclear Threats," April 5, 2011, <https://www.dhs.gov/blog/2011/04/05/dhs-supports-exercise-securing-cities-program-designed-detect-radiological-and> (accessed July 23, 2015).
254. Schafer Corps, "Primary Customer DHS Earns High Praise from Congress," January 21, 2015, <http://www.schafercorp.com/primary-customer-dhs-earns-high-praise-congress/> (accessed July 23, 2015).

255. Government Accountability Office, "DHS Research and Development on Radiation Detection Technology Could Be Strengthened," GAO-15-263, March 2015, <http://www.gao.gov/assets/670/668906.pdf> (accessed September 2, 2015).
256. Steven P. Bucci, "BioWatch: Enhancing Biological Threat Detection," Heritage Foundation *Issue Brief* No. 3661, July 10, 2012, <http://www.heritage.org/research/reports/2012/07/biowatch-enhancing-biological-threat-detection>.
257. Government Accountability Office, "Observations on the Cancellation of BioWatch Gen-3 and Future Considerations for the Program," GAO-14-267T, June 10, 2014, <http://www.gao.gov/products/GAO-14-267T> (accessed July 23, 2015), and David Willman, "Homeland Security Cancels Plans for New BioWatch Technology," *Los Angeles Times*, April 25, 2014, <http://www.latimes.com/nation/la-na-biowatch-20140426-story.html> (accessed July 23, 2015).
258. U.S. Environmental Protection Agency, "ERT and Homeland Security," <http://www.epa.gov/superfund/accomp/news/ert.htm> (accessed June 25, 2015).
259. Federal Emergency Management Agency, "Biological Incident Annex," August 2008, http://www.fema.gov/pdf/emergency/nrf/nrf_BiologicalIncidentAnnex.pdf (accessed June 25, 2015).
260. Paul McHale, "Critical Mismatch: The Dangerous Gap Between Rhetoric and Readiness in DOD's Civil Support Missions," Heritage Foundation *Special Report* No. 115, August 13, 2012, <http://www.heritage.org/research/reports/2012/08/critical-mismatch-the-dangerous-gap-between-rhetoric-and-readiness-in-dod-civil-support-missions>.
261. Coburn, "A Review of the Department of Homeland Security's Missions and Performance," p. 135, and Serbu, "DHS S&T Chief Plans for More Relevant Research, Better Employee Morale."
262. Shea, "The DHS S&T Directorate: Selected Issues for Congress," and Department of Homeland Security, "Apex Programs," April 29, 2015, <http://www.dhs.gov/science-and-technology/apex-programs> (accessed June 25, 2015).



214 Massachusetts Avenue, NE
Washington, DC 20002-4999
(202) 546-4400
heritage.org