Statement for the Record
Robert Kolasky
Director, Executive Order 13636 and Presidential Policy Directive 21 Integrated Task Force
United States Department of Homeland Security
Before the
United States House of Representatives
Committee on Homeland Security
Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies
July 18, 2013

Introduction

Good morning Chairman Meehan, Ranking Member Clarke, and distinguished Members of the Committee. Let me begin by thanking you for your support of the Department of Homeland Security (DHS), particularly in its mission to safeguard and secure the Nation's critical infrastructure. I am pleased to appear before you to discuss the Department's role in implementing Executive Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity*, and Presidential Policy Directive (PPD) 21, *Critical Infrastructure Security and Resilience*.

DHS supports critical infrastructure owners and operators in preparing for, preventing, protecting against, mitigating from, responding to, and recovering from all-hazards events, including cyber incidents, terrorist attacks, and natural disasters. These activities promote the safety and security of the American public and ensure the provision of essential services and functions, such as energy and communications. To achieve this end, DHS works with public and private sector partners to identify and promote effective solutions for security and resilience that address the risks facing the Nation's critical infrastructure.

While this increased connectivity has led to significant transformations and advances across our country – and around the world – it also has increased the importance and complexity of our shared risk. Our daily life, economic vitality, and national security depend on cyberspace. A vast array of interdependent IT networks, systems, services, and resources are critical to communication, travel, powering our homes, running our economy, and obtaining government services. No country, industry, community or individual is immune to cyber risks.

Critical infrastructure is the backbone of our country's national and economic security. It includes power plants, chemical facilities, communications networks, bridges, highways, and stadiums, as well as the federal buildings where millions of Americans work and visit each day. DHS coordinates the national protection, prevention, mitigation, and recovery from cyber incidents and works regularly with business owners and operators to take steps to strengthen their facilities and communities. The Department also conducts onsite risk assessments of critical infrastructure and shares risk and threat information with state, local and private sector partners.

Protecting critical infrastructure against growing and evolving cyber threats requires a layered approach. DHS actively collaborates with public and private sector partners every day to improve the security and resilience of critical infrastructure while responding to and mitigating the impacts of attempted disruptions to the nation's critical cyber and communications networks and to reduce adverse impacts on critical network systems.

Beyond evolving cybersecurity risks, the Nation's critical infrastructure is potentially affected by more frequent and severe weather events, by sustained under-investment in the integrity of aging and degrading infrastructure, and by an evolving terrorist threat.

Recognizing the need for collaborative solutions to confront this changing risk paradigm and promote a more secure and resilient critical infrastructure, President Obama issued EO 13636 and PPD-21. These two directives aim to "enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties."

Taken together, these two policy documents are intended to achieve the following:

- Encourage *the adoption of effective measures across all critical infrastructure sectors to improve security and resiliency and reduce risk from cyber attacks to essential functions and services* by publishing a Cybersecurity Framework (the Framework) that will provide owners and operators with a prioritized, flexible, repeatable, performance-based, and cost-effective set of validated security controls based upon industry best practices.
- Enhance *timely, relevant, and accurate information sharing on significant risks* by implementing a program to develop and rapidly share unclassified information with critical infrastructure owners and operators, enabling the adoption of effective mitigations to prevent or to reduce the consequences of significant incidents.
- Align responsibilities of *public and private partners to efficiently allocate risk reduction responsibilities* by conducting an analysis of the existing critical infrastructure public-private partnership model and recommending options for improving the effectiveness of the partnership in managing both the physical and cyber risks.
- Promote *innovation in novel risk-reduction solutions* by developing a National Critical Infrastructure Security and Resilience Research and Development (R&D) Plan to identify priorities and guide R&D requirements and investments toward those solutions that will help assure the provision of essential functions and services over time.
- Ensure that *privacy, civil rights, and civil liberties are protected as a foundational part of all risk management efforts* by conducting an assessment of the privacy, civil rights, and civil liberties implications of all EO 13636 and PPD-21 programs and recommending revisions to proposed initiatives as required.

Working in partnership with the Federal interagency, DHS established an Integrated Task Force to:

- Lead the Department's implementation of PPD-21 and EO 13636, including coordination with the Department of Commerce's National Institute of Standards and Technology, on the Cybersecurity Framework;
- Serve as the focal point for collaboration with industry;
- Involve key stakeholders from all levels of government; and
- Prioritize tasks, plan implementation, and coordinate principal offices of responsibility.

The Integrated Task Force is further charged with ensuring the production of various deliverables as mandated under EO 13636 and PPD-21. These deliverables, however, are not an end in themselves; rather, each deliverable is intended to contribute to future efforts that will promote the security and resilience of the Nation's critical infrastructure.

Consultative Process

Promoting security and resilience is a collaborative endeavor requiring effort and investment from both the Federal government and private sector, as well as state, local, tribal, and territorial partners. Thus, to implement EO 13636 and PPD-21, the Federal government has actively sought the collaboration, input and engagement of our partners. The Integrated Task Force has developed a "consultative process" pursuant to EO 13636, to work within the Federal government to collaborate with state, local, tribal and territorial government officials as well as private sector owners and operators of critical infrastructure and the non-profit and academic communities. The consultative process is based on the following principles:

- Seek out opportunities across the whole community
- Be systematic, transparent, and repeatable
- Focus on appropriate and meaningful multi-directional communications and collaboration
- Establish protocols to ensure that progress reports, current direction, and current messaging are broadly shared and understood
- Document activities to track participation across the whole community
- Identify and engage the full range of stakeholders across the critical infrastructure and cybersecurity community
- Utilize established partnership organizations and regimes
- Promote innovative approaches to maximize opportunities for input from stakeholders across the whole community
- Ensure that privacy and civil liberties protections are incorporated into the tasks by coordinating with appropriate senior Federal agency officials
- Foster development of an enduring engagement process that can be used in other cyber and critical infrastructure security and resilience efforts

Using those principles, the Integrated Task Force developed nine separate working groups and has conducted more than 100 working sessions involving 1,100 attendees, to date. Representatives from DHS have also conducted more than 100 briefings on our efforts to nearly 10,000 stakeholders since February 2013. Outside of the established Integrated Task Force working groups, the cyber and critical infrastructure communities are being engaged through working sessions, conferences, meetings, and virtual collaboration methods such as the Homeland Security Information Network, IdeaScale, and webinars. The format and style of engagement varies according to the needs of the community engaged and the purpose for engagement. The venue and mechanism for engagement is also determined by the outcomes sought and the nature of the constituency involved. In addition, DHS has worked with the Department of Commerce's National Institute of Standards and Technology (NIST) to utilize the consultative process in support of the development of the Framework.

Status of Current Efforts

We have accomplished much over the past 150 days using the Consultative Process to engage whole community stakeholders. The Secretary has already submitted several EO 13636 and PPD-21 deliverables to the White House, to include:

- An Incentives Report, which analyzes potential government incentives that could be used to promote the adoption of the Framework;
- A description of critical infrastructure functional relationships, which illustrates the Federal government's current organizational structure to deliver risk management support to stakeholders and make it easier for them to collaborate with the government;
- Instructions on producing unclassified cyber threat reports from all sources of information, including intelligence, to improve the ability of critical infrastructure partners to prevent and respond to significant threats;
- Procedures for expansion of the Enhanced Cybersecurity Services (ECS) program to all critical infrastructure sectors. The ECS program promotes cyber threat information sharing between government and the private sector, which helps critical infrastructure entities protect themselves against cyber threats to the systems upon which so many Americans rely. DHS will share with appropriately cleared private sector cybersecurity providers the same threat indicators that we rely on to protect the .gov domain. Those providers will then be free to contract with critical infrastructure entities and provide cybersecurity services comparable to those provided to the U.S. Government;
- Recommendations on feasibility, security benefits and merits of incorporating security standards into acquisition planning and contract administration, addressing what steps can be taken to make existing procurement requirements related to cybersecurity consistent;
- A process for expediting security clearances to those in the private sector with an essential "need to know" regarding classified cybersecurity risk information. This processing is intended only for those who need access to classified information. While it is important to ensure that our private sector partners who have a valid need for access to classified information receive appropriate security clearances, we believe that most information sharing can be conducted at the unclassified level; and
- A report outlining how well the current critical infrastructure public-private partnership model as articulated in the National Infrastructure Protection Plan (NIPP) is working toward promoting the security and resilience of the Nation's critical infrastructure, and recommendations to strengthen those partnerships.
- In addition, we have conducted an initial evaluation of and are identifying critical infrastructure entities which would reasonably result in catastrophic consequences from a cybersecurity incident. While we are incorporating lessons from this analysis in developing a repeatable system of critical infrastructure assessments, the results from this preliminary evaluation identified a relatively small list of U.S. critical infrastructure that if impacted by a cybersecurity incident could cause catastrophic consequence to our national security, economic security, public health and safety.

Moving Forward

While we have made significant progress to date, there is much work still to be done this year to fulfill the vision set forth in EO 13636 and PPD-21. To that end, DHS will be focusing its efforts on the following steps via the Integrated Task Force:

- Updating the NIPP to reflect new policies, a change in the risk environment, and lessons learned working in collaboration across the public and private sectors to manage infrastructure risk;
- Enhancing near real-time situational awareness for critical infrastructure, with a particular focus on multi-directional information sharing and understanding of interdependencies between physical and cyber systems and critical infrastructure sectors;
- Developing a draft of the National Critical Infrastructure Security and Resilience Research and Development Plan; and
- Collaborating with NIST on the Cybersecurity Framework.

DHS is developing the Performance Goals described in EO 13636 for the Framework collaboratively with critical infrastructure owners and operators using the Consultative Process. By framing the importance of cyber risk in a business context, the Performance Goals will encourage adoption of the Framework. The goals complement the Framework which will outline *what* businesses should do to manage cyber risk. In turn, the specific standards and controls suggested under the Framework will explain *how* businesses should manage cyber risk.

Through the Performance Goals, critical infrastructure owners and operators will be able to adopt a common approach to evaluating the effectiveness of risk management investments based upon business outcomes. While DHS will not require nor evaluate the adoption of the Performance Goals among critical infrastructure owners and operators, the Goals will encourage businesses to frame cybersecurity risk in the context of economic sustainability, and thereby facilitate strategic planning and investment to identify changing risks and implement measurably effective solutions.

The Framework will also serve as a basis for a DHS Voluntary Program, which will result in ongoing collaboration with industry to promote market-based solutions to higher levels of cybersecurity.

Cyber Legislative Priorities

It is important to note that EO 13636 directs Federal agencies to work within current authorities and increase voluntary cooperation with the private sector to provide better protection for computer systems critical to our national and economic security. We continue to believe that a comprehensive suite of legislation is necessary to implement the full range of steps needed to build a strong public-private partnership, and we will continue to work with Congress to achieve this.

Consistent with the proposal that the Administration transmitted last Congress, legislation should:

- Facilitate cybersecurity information sharing between the government and the private sector as well as among private sector companies. We believe that such sharing can occur in ways that uphold privacy and civil liberties protections, expand upon existing best practices from industry leaders in this area, reinforce the appropriate roles of intelligence and non-intelligence agencies, and include targeted liability protections;
- Incentivize the adoption of best practices and standards for critical infrastructure by complementing the process set forth under the Executive Order;
- Give law enforcement the tools to fight crime in the digital age;
- Update Federal agency network security laws, and codify DHS' cybersecurity responsibilities; and
- Create a National Data Breach Reporting requirement.

In each of these legislative areas, we want to incorporate robust privacy and civil liberties safeguards. The Administration stands ready to work with Congress to pass important cybersecurity legislation.

Conclusion

Critical infrastructure security and resilience to cyber incidents and other risks is an ongoing capability development effort rather than an end state to be achieved on a given date, or via a defined deliverable. All partners in this national effort will need to continue to contribute to its progress over time. The implementation of EO 13636 and PPD-21 is a key step in achieving these desired outcomes; progress will require sustained effort by both public and private partners, and a recognition of the rapidly evolving risk environment. The desired end-state of the critical infrastructure partnership model is an environment in which public and private partners work in a networked manner to effectively and efficiently share information and allocate risk-reduction responsibilities. If achieved, this result will maximize the comparative advantage of each and reduce duplication or under-investment, resulting in collaborative solutions to reduce the likelihood of the highest-consequence incidents.

Thank you for the opportunity to discuss the Department's role in improving critical infrastructure security and resilience. I look forward to any questions you may have.