Critical Infrastructure Activities

September 30, 2015

Fiscal Year 2015 Report to Congress

Homeland Security

National Protection and Programs Directorate

Message from the Under Secretary

September 29, 2015

I am pleased to present the following report, "Critical Infrastructure Activities," prepared by the National Protection and Programs Directorate (NPPD).

This document has been compiled pursuant to a requirement in House Report 113-481, which accompanies the *Fiscal Year 2015 Department of Homeland Security Appropriations Act* (P.L. 114-4). This report outlines NPPD's current activities and plans to address the following issues: 1) enhanced engagement with private sector owners and operators; 2) robust, near-real time information-sharing mechanisms; 3) collaboration with universities, industry, and government labs; and 4) integration of its programs and capabilities.

In accordance with congressional requirements, this report is being provided to the following Members of Congress:

The Honorable John R. Carter
Chairman, House Appropriations Subcommittee on Homeland Security

The Honorable Lucille Roybal-Allard
Ranking Member, House Appropriations Subcommittee on Homeland Security

The Honorable John Hoeven
Chairman, Senate Appropriations Subcommittee on Homeland Security

The Honorable Jeanne Shaheen
Ranking Member, Senate Appropriations Subcommittee on Homeland Security

If you have any questions, please do not hesitate to contact me at (703) 235-1934 or the Department's Deputy Under Secretary for Management and Chief Financial Officer, Chip Fulghum, at (202) 447-5751.

Sincerely,

Suzanne Spaulding
Under Secretary
National Protection and Programs Directorate

Executive Summary

The National Protection and Programs Directorate (NPPD) leads the national effort to secure and enhance the resilience of the Nation's infrastructure against physical and cyber risks. To carry out its mission, NPPD must be nimble to respond quickly to ongoing incidents while maintaining steady-state operations, providing critical services to stakeholders, and carrying out its strategic mission. Critical infrastructure security and resilience efforts must address all hazards - from terrorism and other criminal activities to natural disasters and cybersecurity threats.

This report outlines the current activities and plans to achieve the mission, specifically addressing:

1. Enhanced engagements with private sector owners and operators by institutionalizing and streamlining strategic and operational processes and by establishing continuous feedback and measurement mechanisms to enable NPPD to strengthen its partnerships, add value to its customers, and continue to evolve and adapt to the changing risk landscape.
2. The facilitation of robust, near-real time information sharing through existing information-sharing mechanisms by supporting sector-specific Information Sharing and Analysis Centers and promoting Information Sharing and Analysis Organizations.
3. Continued collaboration with universities, industry, and government, including the potential to establish a large-scale test-bed to facilitate research, test new concepts, and train personnel to improve readiness and response to natural disasters.
4. The need for organizational improvements and integration of programs and capabilities in order to fully address the current risk landscape and ensure effective and efficient mission operations.

The project activities and recommendations described in the report are essential to the larger Department of Homeland Security mission to build a resilient Nation, safeguard and secure cyberspace, and strengthen the security enterprise.

Critical Infrastructure Activities

Table of Contents

I. Legislative Language

House Report 113-481, which accompanies the *Fiscal Year* (FY) *2015 Department of Homeland Security* (DHS) *Appropriations Act* (P.L. 114-4), includes the following requirement:

> The Committee directs the National Protection and Programs Directorate (NPPD) to provide a report, not later than 90 days after the date of enactment of this Act, with the following:
>
> 1. NPPD's plans to better understand and respond to the full range of critical infrastructure risk through enhanced engagement with private sector owners and operators of such infrastructure.
>
> 2. Recommendations to provide compensation to owners of critical infrastructure for services and hardware incurred in the act of information sharing, analyzing, or exercising with any DHS agency or instrument regarding critical infrastructure protection as referenced in this paragraph.
>
> 3. A description of all current and planned collaborative ventures between NPPD and universities, industry, and government labs to address critical infrastructure risk, including a recommendation on the feasibility and merit of establishing a large-scale test-bed to facilitate research, test new concepts, and train personnel to improve readiness and response to natural disasters and cyber-physical attacks on the electrical grid.
>
> 4. An assessment of the need for a revised organizational structure to better align the agency's critical infrastructure protection activities across cyber, physical, and human risks, including those protecting government facilities and networks.

II. Background

The Nation's well-being is dependent upon a secure and resilient critical infrastructure. These assets, systems, and networks are key components that underpin American society. The National Protection and Programs Directorate (NPPD) supports all of the homeland security missions outlined in the Quadrennial Homeland Security Review; however, NPPD's primary mission is to lead the national effort to strengthen the security and resilience of the Nation's critical infrastructure against cyber and physical risks. This mission includes strengthening the security and resilience of Federal facilities and Federal civilian (.gov) networks, protecting critical infrastructure, and strengthening cybersecurity. Other layers of this multifaceted mission include ensuring emergency communications through a full spectrum of conditions, and delivering enterprise identity services that enable and support homeland security missions. Finally, NPPD shares information and collaborates with, and provides response, mitigation, risk management, and analysis capabilities to Federal, state, local, tribal, and territorial government and private sector partners.

NPPD is uniquely qualified to accomplish this mission and deliver value to the Nation through an array of efforts, including evolving relationships with critical infrastructure owners and operators in the public and private sectors. Additionally, NPPD possesses the ability to aggregate and share information and conduct analysis, which informs risk management decisions. NPPD builds the capacity of critical infrastructure owners and operators, and state and local government partners to mitigate the risk of debilitating and catastrophic incidents to further accomplish its mission. NPPD is well-equipped to scale security solutions across the critical infrastructure sectors and jurisdictional boundaries while incentivizing innovative solutions.

III. Enhanced Engagement with Private Sector Owners and Operators

The Nation's critical infrastructure continues to face risks ranging from cyber criminals and hackers to natural disasters and industrial accidents. The effort to reduce the risk to our critical infrastructure has been a joint effort between the private and public sectors, largely supported in a voluntary context under the *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* (NIPP), and primarily focused on the protection of systems and assets. The NIPP defines the sector partnership model as "the framework used to promote and facilitate sector and cross-sector planning, coordination, collaboration, and information sharing for critical infrastructure protection, involving all levels of government and private sector entities." NPPD leads the national effort to coordinate government and private sector-specific councils and various cross-sector councils that enable government and private sector partners to engage in joint discussions and participate in a broad spectrum of activities. NPPD also has a large cadre of employees in the field who routinely engage with critical infrastructure owners and operators to further NPPD's mission to provide situational awareness, to help build capabilities to manage risk and to protect infrastructure.

The evolving nature of the threat to critical infrastructure, as well as the maturation of the critical infrastructure partnership, necessitates a shift from a focus on individual asset protection to one of overarching system and network security and resilience from all threats and hazards. In addition, many critical infrastructure owners, operators, and vendors have taken advantage of the substantial cost and operational efficiencies that information and communications technologies offer. While having benefits, this emerging dependence on automation and the increasing virtual interconnectedness of previously isolated and manual systems also creates new and additional vulnerabilities. The critical infrastructure partnership must continue to evolve if it is to successfully address these vulnerabilities now and in the future.

Overall, the desired end-state of NPPD's partnership is an environment in which public and private partners work in a networked manner to share information and allocate risk-reduction responsibilities effectively and efficiently. The outcome of enhanced engagement will maximize the comparative advantage of each partner and reduce duplication or under-investment, resulting in collaborative solutions that reduce the likelihood of high-consequence incidents.

NPPD's Private Sector Engagement

To accomplish the vision laid out in the NIPP, NPPD conducts extensive private sector engagement across the organization for the purpose of building relationships, sharing

information, and assisting in capacity building. NPPD is required, by statute and by Executive Order (E.O.), to engage domestic and international partners at all levels of government and the private sector. This engagement increases preparedness for all hazards and enhances the security and resilience of infrastructure to cyber and physical risks. This includes coordination with Federal agencies; regional coordination with State, local, tribal, and territorial governments and the private sector; and international and national-level coordination through established councils and associations.

NPPD employees have spent years establishing partnerships with private and public sector partners in their particular mission areas and building trust in order to share information. Employees across the organization are respected and trusted by their colleagues in the public and private sectors. There is an opportunity to take greater advantage of these existing relationships across the entire mission areas, regardless of origin, by evaluating relationship management practices and leveraging existing business practices and staffing associated with that work. NPPD is committed to leveraging opportunities for enhancement and mission synergies that currently may be missed or unrealized in the current construct.

NPPD's Vision and Plan for Enhanced Private Sector Engagement

The vision for enhancements to NPPD's private sector engagement function is to develop a more integrated, organization-wide strategy for accomplishing NPPD's multifaceted mission and to ensure that the approach to private sector engagement reflects NPPD's evolving mission. Recent examples demonstrate that integration across NPPD programs is an effective way of achieving results and meeting the needs of stakeholders. Both the joint implementation effort of the E.O. on Improving Critical Infrastructure Cybersecurity and Presidential Policy Directive (PPD) 21, *Critical Infrastructure Security and Resilience*, as well as the implementation of E.O. 13650, *Improving Chemical Facility Safety and Security*, prove that integrated private sector engagement results in success. During the implementation of the Cybersecurity E.O. and PPD on Critical Infrastructure Security and Resilience, an integrated task force was established with representatives from across NPPD, as well as from other DHS and interagency partners. The task force ensured that activities in support of implementation were carried out to support the goals of the documents and that feedback from private sector stakeholders was coordinated. Similarly, during implementation of E.O. 13650, integrated implementation within NPPD and among interagency partners resulted in cohesive results and reduced duplicative engagement with stakeholders that would have occurred if the agencies were responsible for implementing the E.O. alone.

To help achieve this vision, NPPD established a working group of leaders within the organization who work regularly with private and public sector partners to develop a plan with regard to NPPD's customer engagement activities to:

- Achieve a greater unity of effort across NPPD;
- Ensure effective operations and management of NPPD's programs; and
- Leverage partnerships and drive innovation to enhance security and resilience.

The working group focused on finding balance among the following:

- Creating a champion for overall customer engagement, without adding a burdensome layer;
- Identifying processes to streamline engagement but not lose the value of components and programs working with customers directly;
- Appreciating the nuances/regional customization of the Components' customer engagements and relationships while recognizing and capitalizing on the similarities;
- Investing in new tools and processes while identifying low-cost, more easily accomplished (given current authorities and structures) solutions to improving customer engagement synchronization and responsiveness; and
- Building approaches to share information quickly and flexibility to anticipate emerging risks and risk management requirements.

Using this framework, NPPD has adopted a plan to enhance private sector engagement over the next year, which includes eight action items:

- **Action Item 1:** Appoint NPPD Customer Engagement Lead and Supporting Governance Body.
- **Action Item 2:** Establish Strategic Planning Process for Customer Engagement.
- **Action Item 3:** Establish Common Set of Customer Engagement/Satisfaction Metrics and process for getting feedback from non-Federal partners.
- **Action Item 4:** Integrate select Customer Engagement "Support Mechanisms" to achieve economies of scale.
- **Action Item 5:** Build an NPPD Customer Relationship Management System based on defined requirements.
- **Action Item 6:** Establish Customer Engagement/Service Culture.
- **Action Item 7:** Establish a Regional Integration Pilot to assess the benefits of better integrating NPPD field staff.
- **Action Item 8:** Develop and Implement Regional Engagement Strategies that prioritize engagement efforts to reduce and mitigate risks specific to the region.

Information Sharing

NPPD is committed to improving two-way information sharing with the private sector. Leveraging the NIPP partnership model, NPPD shares information with critical infrastructure owners and operators to prevent, prepare for, and respond to all types of

incidents, including natural disasters, terrorist threats, cyber attacks, pandemics, and transnational crimes that could that could potentially affect essential services. NPPD serves as a convening body to promote enhanced cooperation, as well as provides tools and training to help its partners manage risks to their assets, systems, and networks.

Additionally, in accordance with PPD-21, NPPD is working to integrate the information-sharing mechanisms of the National Infrastructure Coordinating Center (NICC) and the National Cybersecurity and Communications Integration Center (NCCIC) to obtain enhanced situational awareness and provide integrated, actionable information. Information sharing relies heavily on voluntary collaboration with private sector partners to execute an integrated cycle of planning, training, exercises, and incident management activities. Leveraging these operational centers, NPPD works to maintain shared situational awareness among partners that furthers national protection, improves prevention and mitigation efforts, and supports recovery activities associated with significant incidents.

To enhance the value of the information shared by partners, NPPD has enhanced analytic capabilities of the Office of Cyber and Infrastructure Analysis, which is the Federal Government's foremost hub for identifying the consequences to the Nation's critical infrastructure from cyber and physical incidents. That analysis gives NPPD an ability to pinpoint mitigation opportunities and use its programs to engage with the private sector to address critical infrastructure risks.

Path Forward

Over the next year, NPPD will work in concert with its internal and external stakeholders to improve engagement and enhance information sharing and shared situational awareness. These action items, when implemented, will help NPPD to institutionalize and streamline the strategic and operational processes to better serve its private sector partners as well as to deepen its understanding of risks to critical infrastructure. Continuous feedback and measurement mechanisms will enable NPPD to strengthen its partnerships, add value to its customers, and continue to evolve and adapt to the changing risk landscape.

NPPD is implementing the Call to Action in the 2013 NIPP to strengthen engagement with critical infrastructure owners and operators by building on partnership efforts, particularly those that:

- Set national focus through jointly developed priorities
- Determine collective actions through joint planning efforts
- Empower local and regional partnerships to build capacity nationally
- Leverage incentives to advance security and resilience

NPPD also has broadened the aperture to work more closely with other private sector groups, such as regional consortia and coalitions, including Information Sharing and Analysis Organizations (ISAO).

NPPD is emphasizing work outside of the Washington, D.C., area, using field forces across NPPD to work directly with critical infrastructure owners and operators, including Federal facilities, and the state, local, tribal, and territorial government partners that help to provide local protection and response. NPPD's Protective Security Advisors, Cyber Security Advisors, Chemical Security Inspectors, Federal Protective Service officers, and Emergency Communications Coordinators have been working to bring greater visibility across those forces in the field about each other's activities so that they can leverage each other's relationships, expertise, and insight better to accomplish the overarching mission of strengthening the security and resilience of critical infrastructure. NPPD's plan, as more fully described in Section IV, is to provide the institutional structure that reinforces and supports this field-based operational activity.

IV. Costs and Benefits for Critical Infrastructure Owners and Operators

Background

Today's critical infrastructure risks extend beyond the ability of individual companies or even whole industries to address necessitating strong partnerships. During major incidents, owners and operators must work seamlessly across sectors and with the government to respond and recover rapidly. Achieving this level of coordination in advance requires strong relationship building from the national to the local levels. Thus, the public and private sectors must work together to protect the Nation's critical infrastructures better and the vital services that the infrastructures support. Private sector security investments, while essential, must demonstrate a clear value proposition to justify the costs in a highly competitive and resource-constrained business environment. Investment decisions must be risk-based.

While individual companies are responsible for the execution of their own security programs, the overall security of the Nation's critical infrastructure is a shared responsibility. Within this context, the Federal Government is uniquely positioned to work with private critical infrastructure owners and operators. NPPD facilitates these public-private partnerships, which create the foundation for stakeholders to share information, characterize their risks, make informed investments, train staff, exercise response procedures, and ultimately build security and resilience into U.S. critical infrastructure. NPPD leads the national effort for the voluntary public-private partnership, outlined by PPD-21, *Critical Infrastructure Security and Resilience*, and furthered by the partnership framework outlined in the NIPP.

The NIPP and Public-Private Information-Sharing and Coordination

The NIPP lays out the national-level strategic framework for the public and private sectors to work together toward achieving critical infrastructure security and resilience. It organizes the Nation's critical infrastructure into 16 sectors, identifies Sector-Specific Agencies for each of the sectors, and establishes the requirement for partnerships of the Federal Government, critical infrastructure owners and operators, and State, local, tribal, and territorial government entities. The NIPP defines the partnership structure as "the framework used to promote and facilitate sector and cross-sector planning, coordination, collaboration, and information sharing for critical infrastructure protection, involving all levels of government and private sector entities."

Per the NIPP, Sector Coordinating Councils, consisting of non-Federal owners, operators, and trade associations, serve as the primary private sector interface with the Federal Government. Sector Coordinating Councils work closely with their Federal counterparts, the Government Coordinating Councils. Government Coordinating Councils include representatives from Federal, state, local, tribal, and territorial entities and work to facilitate interagency and cross-jurisdictional coordination within a sector. The sector and cross-sector partnership approach outlined in the NIPP is designed to be scalable and to allow individual owners and operators of critical infrastructure and other stakeholders across the country to participate voluntarily. It is intended to promote consistency of process to enable efficient collaboration between disparate parts of the critical infrastructure community, while allowing for the use of other viable partnership structures and planning processes.

As discussed in the NIPP, information sharing is a key crosscutting element of the risk management framework. The NIPP promotes Federal and private sector organizations to share information within and across sectors, as well across the public and private domains. Information Sharing and Analysis Centers (ISAC) are one of these key information sharing mechanisms, voluntarily formed and self-organized by critical infrastructure owners and operators. ISACs vary by sector, but often provide 24/7 threat-warning and incident-reporting capabilities, as well as security-related best practices. ISACs have the ability to gather, analyze, and share threat and vulnerability information within and among sector, private stakeholders, and the government. Government entities rely on ISACs for situational awareness and to provide timely and actionable data to their stakeholders.

ISAOs, originally identified in the Homeland Security Act of 2002 and furthered by the NIPP, are more broadly defined as public or private sector information-sharing bodies used to exchange critical infrastructure information. More recently, however, E.O. 13691, *Promoting Private Sector Cybersecurity Information Sharing*, identifies ISAOs to serve as the focal point for cybersecurity information sharing between the private sector and the government. ISAOs may be organized by sector, subsector, or geographic region and membership is open to entities (nonprofit and for-profit) from any and all sectors. E.O. 13691 also tasked NPPD's NCCIC with continuous engagement and collaboration with ISAOs in sharing information related to cybersecurity risks and incidents.

The Benefits and Costs of the Public-Private Partnership Framework

The NIPP partnership model is strictly voluntary for the private sector and does not provide financial compensation for participation. In keeping with the voluntary nature of the program, however, the NIPP partnership model also does not require any hardware, tools, or other purchases in order to participate.

Furthermore, DHS does not have the authority to provide direct monetary support to private sector entities participating in coordination entities established under the NIPP. As a result, private sector individuals and companies do bear some financial costs associated with travel to attend meetings. DHS does have authority to provide funding to support some limited travel for public sector stakeholders. Invitational travel funding is provided to State, Local, Tribal, and Territorial Government Coordinating Council representatives so that they may participate in sector forums, where they articulate shared critical infrastructure security and resilience priorities and current state, local, tribal, and territorial activities underway, and provide insights and recommendations from a state, local, tribal, and territorial perspective to the Federal Government in order to form positions and make policy decisions. Travel amounts provided for FY 2015 to date total $41,000.

On average, more than 200 meetings within and across sectors occur each year, with participants from more than 3,500 public and private partners. In 2014, there were more than 350 sector-specific meetings with roughly 5,000 stakeholders, and 97 sector-specific conferences, industry meetings, and events with more than 1,200 participants. While each sector has multiple working groups, there are some common ones across the sectors, such as information sharing and cybersecurity. All sectors form their own initiatives and projects, loosely outlined in their sector–specific plan. Additionally, in 2014, there were 70 cross-sector council meetings and 100 events that were held under the Critical Infrastructure Partnership Advisory Council (CIPAC), a legal framework that enables government and private sector partners to engage in joint critical infrastructure security and resilience-related discussions. Currently, NPPD provides administrative support to the 16 sectors under the auspices of the CIPAC. On request, NPPD provides limited administrative support to the Sector Coordinating Councils for which DHS has responsibility.

The benefits of the NIPP partnership accrue to both private sector companies and to the broader community. In addition to providing private businesses access to Federal information, tools, and resources, public-private partnerships also help to contribute to improving critical infrastructure security and resilience through policy coordination, joint planning, information sharing, shared risk and incident management, and joint investment. For example, ISACs and ISAOs provide owners and operators with access to actionable information, comprehensive threat and incident analysis, and the ability to maintain collaborative relationships with the Federal Government, specifically operational centers such as the NICC and the NCCIC. This coordination assists the private sector in gaining a more comprehensive picture of the risk landscape, enhancing the ability to make informed and effective investments.

These partnerships also facilitate enhanced security measures at specific assets, benefiting individual companies, as well as at a systemic level to enhance national-level security and resilience. For example, many stakeholders operate solely within their

industry or facility and may not be fully aware of other sector dependencies and cascading impacts. The Regional Resiliency Assessment Program (RRAP) is a cooperative, voluntary, NPPD-led assessment of both specific critical infrastructure and a regional analysis of the surrounding infrastructure. The RRAP provides an analysis and addresses hazards of regional and national significance. The RRAP also incorporates vulnerability assessments, capabilities assessments, and infrastructure protection planning efforts to assemble an analysis of a region's critical infrastructure and relevant preparedness capabilities. Private sector stakeholders involved in the RRAP process are informed of interdependencies and cascading impacts involving their facility that may not have been apparent prior to the assessment.

Complementary to the RRAP is the Infrastructure Survey Tool (IST) security assessment. The participating private sector facility receives a report and interactive dashboards that include comparative security and resilience information and options for consideration to close security and resilience gaps at their facility. Private sector owners and operators participate in the information sharing and gathering interviews for each of these assessments. The resource levels provided by the private sector can vary by the facility's involvement. Typically, the assessment is conducted at the facility, so there is no travel cost for the private owner. The facility being assessed will provide space for the interview to take place and the time of its appropriate staff. There is no requirement as to how many facility personnel must take part in the assessment; the key is to ensure that NPPD is able to get the appropriate information needed to make an assessment. NPPD provides expert personnel utilizing a uniform assessment methodology for the assessments. Following the assessment, NPPD directs the private owner/operator to any appropriate Federal resources that may be applicable. In Fiscal Year 2014, NPPD initiated 10 RRAP projects (increased to 12 for FY 2015) and 621 IST security surveys.

Cybersecurity Coordination and Associated Costs and Benefits

Now more than ever, public-private partnerships are necessary to address evolving cybersecurity issues. As seen in several highly publicized cyber incidents, a breach at a large private retailer can impact thousands of public citizens by compromising valuable personal information. By providing cyber threat and incident information, as well as tools to secure systems, both private industry and the American public are better protected against cyber crimes. NPPD's Critical Infrastructure Cyber Community Voluntary Program is an example of a federal program that provides industry access to free and readily available technical assistance, tools, and resources to strengthen capabilities to manage cyber risks.

The Cyber Information Sharing and Collaboration Program (CISCP) is another example of a program that benefits both the private sector and the American public. This program establishes a common operational picture accessible to both public and private entities, by aggregating and analyzing information shared among trusted partners. The program

helps to facilitate protective actions, mitigation efforts, and coordination necessary for an efficient and effective response to cyber and/or communications threats and incidents. For all CISCP meetings, NPPD provides the facility, meeting equipment, and work group management support. The private sector provides personnel and travel as needed.

Furthermore, through NPPD's National Cyber Exercise and Planning Program (NCEPP), the private sector works with public partners to discuss key issues and build and test processes for government and private sector to respond collaboratively to cybersecurity incidents. The NCEPP conducts an average of 9 exercises per year with heavy private sector participation, resulting in more than 50 individual private sector companies participating in NCEPP-led exercises. In support of these exercises, NPPD typically provides planning meeting support and facilitation, which can include meeting agenda and minutes development. Additionally, NPPD provides financial support to send exercise planners to travel for exercise facilitation and execution (if conducted outside of the National Capital Region).

V. Current and Planned Collaborative Ventures with Universities, Industry, and Government Labs

NPPD has been working with universities, such as Carnegie-Mellon, James Madison University, George Mason University, and others to better understand cyber and physical risks to critical infrastructure and to promote education in this area. NPPD has worked extensively with the private sector through coordinating councils, engagement forums, and local contact by NPPD advisors in the field. NPPD has a long-established relationship with Federally Funded Research and Development Centers (FFRDC) grounded in the Homeland Security Act of 2002. NPPD will continue to develop these relationships in the future. A summary of key relationships is described in Table 1.

Table 1. Key FFRDC, University, Industry, and NPPD Relationships for Critical Infrastructure Risk

FFRDC	Universities	Industry	NPPD Activity
Los Alamos National Laboratory (NL)	Quantum Key Distribution (University of Illinois)		
Sandia NLs			Chemical Economic Criticality Analysis (Office of Infrastructure Protection, or IP) NCCIC Industrial Control Systems Computer Emergency Response Team (ICS-CERT) Tools (Office of Cybersecurity & Communications, or CS&C) Network Security Deployment (Architecture, Managed Security Services, Analytics, Interagency Vision) (CS&C) Federal Network Resilience Continuous Diagnostics & Mitigation (CS&C) Stakeholder Engagement and Cyber Infrastructure Resilience Supply Chain Risk Management (CS&C) National Infrastructure Simulation and Analysis Center Collaboration (Office of Cyber and Infrastructure Analysis (OCIA)) Prioritization and Modeling (OCIA) Strategic Infrastructure Analysis (OCIA)

FFRDC	Universities	Industry	NPPD Activity
Idaho NL			ICS-CERT Incident Response, Workforce Development, Cybersecurity Assessments, Assessment Tools (CS&C) DHS RRAP (IP)
Pacific Northwest NL	Collaboration to facilitate research and test new concepts	Collaboration to train personnel in support of Emergency Support Function 12 International Training Support	Climate Change and Energy Infrastructure (OCIA) Smart Grid Technology Risks (OCIA)
Argonne NL	Cyber Resilience Review (Carnegie Mellon University) CS&C Internet Scale Attack and Event Generation Environment (Iowa State University)	Collaboration on RRAP	IP Gateway Deployment (IP) RRAP Implementation (IP) Technical Support (OCIA) Enterprise Geographic Information System Support (OCIA) Cyber Infrastructure Survey Tool (CS&C) Risk Analysis Training (OCIA and SL Fusion Centers)

A large-scale test-bed to facilitate research, test new concepts, and train personnel to improve readiness and respond to natural disasters and cyber-physical attacks on the electrical grid is feasible, utilizing existing capabilities within academia and national laboratories. While much work currently is being accomplished by these entities for critical infrastructure risk, there could be improvements in both economies of scale and scope if they were coordinated by a central roadmap.

Currently no Federal department or agency, including the Department of Energy (DOE), is in direct possession of cyber-physical test-beds. However, DOE utilizes existing test-beds funded via competitive contracts, and some Department components have created partnerships with institutions that have them (i.e., Homeland Security Advanced Research Projects Agency and Defense Technology Experimental Research test-bed). Limited information was available regarding test-bed production and operations to include in this response.

There are several capabilities housed within NPPD that could be leveraged in a test-bed environment. Notably, the Federal Protective Service (FPS) Center of Excellence at the Federal Law Enforcement Training Center (FLETC) is collaborating with various national-level critical infrastructure partners to establish a Protection Center of

Excellence. The overarching objective of the Protection Center of Excellence is to develop a Corps of Protection Professionals who are deeply skilled, educated, and trained in critical infrastructure protection competencies across all security sectors (government and private sector inclusive). This resource will be available to strengthen organizations responsible for the security and resilience of the Nation's critical infrastructure.

NPPD is partnering with FLETC to leverage its successful approach to standardize basic federal law enforcement training. Other partners include the DHS Transportation Security Administration, Department of Justice, Department of Defense (DOD), and numerous Interagency Security Committee member agencies. The Interagency Security Committee has established a working group to develop the Protection Center of Excellence scope and concept further, and the group is proceeding with a needs analysis associated with the security specialist competencies.

Additionally, during FY 2012 and FY 2013, FPS partnered with DHS Science &Technology (S&T) on a project aimed at developing a technical specification for a threat analytic system to support FPS's threat management requirements. This project delivered a strategic organizational analysis of the threat management process in FPS, a data sources report, an evidence assessment of FPS's use of security countermeasures, and a technical specification for a threat analytic system. The performers utilized to produce the project deliverables included Research Triangle Institute International, the Naval Research Laboratory, and George Mason University.

Based on an assessment of several DOE national labs' (Argonne, Idaho, Los Alamos, Pacific Northwest, and Sandia) current capabilities, it may be possible to establish a large-scale test-bed to facilitate research, test new concepts, and train personnel to improve readiness and respond to natural disasters. A brief description of each lab's capabilities to enable a large-scale test-bed follows, with greater detail included in Appendix A.

- **Los Alamos National Laboratory** focuses on researching quantum key distribution to exchange cryptographic keys ultimately to encrypt energy sector information.
- **Sandia National Laboratories** conducts research and development to address cyber-physical risk to critical infrastructure systems by deploying physical test-beds and extensions of these test-beds via virtualized environments to test, evaluate, train, and exercise.
- **Idaho National Laboratory** closely resembles the concept of a national cyber-physical infrastructure test-bed. Key features of this test-bed include the National Electric Grid Reliability test-bed, the National Wireless test-bed, and the National Supervisory Control and Data Acquisition (SCADA) test-bed. Idaho National Lab is also developing a methodology to allow energy sector stakeholders to analyze

technical, cybersecurity threat information and understand how those threats affect their overall risk posture.

- **Pacific Northwest National Laboratory's** work in cyber-physical systems spans from the facilitation of scientific research to implementation and operation through several research-scale test-beds. The lab has three research test-beds that are used for research, development, testing, evaluation, and training.
- **Argonne National Laboratory** has a particular focus on resilience research for the grid and for the rest of the Nation's infrastructure. Argonne currently is developing a concept for a national Resilient Design User Facility, which would give researchers access to its physical science and computing facilities to test and simulate the resiliency of key infrastructure systems.

VI. The Need for a Revised Organizational Structure

Background: NPPD Organizational Structure

NPPD was created on March 31, 2007, via DHS's authority under Section 872 of the Homeland Security Act of 2002 (P.L. 107-296). Upon its creation, NPPD was comprised of CS&C, IP, the Office of Risk Management and Analysis (RMA), the Office of Intergovernmental Programs (IGP), and United States Visitor and Immigrant Status Indicator Technology (US-VISIT).

Over the years, various pieces of the organization have been transitioned out of the organization (RMA and IGP) or have been altered (US-VISIT became Office of Biometric and Identity Management [OBIM] at the direction of Congress). NPPD also assumed responsibility for FPS and established OCIA. Most significantly, NPPD has grown from a headquarters component of a few hundred to an operational entity with a workforce of more than 3,000 Federal employees and approximately 15,000 contractors located throughout the Nation. To accomplish this dramatic increase in operational activity effectively, NPPD must transition from a headquarters entity to an operational component to lead the national effort to secure and enhance the resilience of the Nation's critical infrastructure against cyber and physical risks.

In addition, the growing complexity and convergence of risks facing critical infrastructure require that NPPD better integrate its efforts across the organization to carry out its mission more effectively and efficiently. Growing interdependencies between cyber and physical infrastructure have increased the potential risk and consequences of incidents to the Nation's critical infrastructure. NPPD must be nimble with the capability to respond quickly to ongoing incidents while maintaining steady state operations, providing critical services to stakeholders, and carrying out its strategic mission. Additionally, the threat and risk landscape has evolved significantly since the creation of the Department. Critical infrastructure security and resilience efforts must address all hazards (from terrorism and other criminal activities to natural disasters to cybersecurity threats), take into consideration aging and failing infrastructure, and address climate change appropriately. NPPD was not organized with this evolving strategic environment in mind and needs to align to fully address the current landscape and its strategic mission.

Keeping pace with evolving threats and hazards also requires taking advantage of technology innovation. NPPD must ensure that its major acquisitions are accomplished with the required agility and in a manner that is efficient and effective.

Enhanced Integration of NPPD Programs

In May 2014, NPPD assembled a task force to assess the need for organizational change. The task force determined that an assessment for organizational change would be a longer effort, but that there were several steps that NPPD could take in the interim to better integrate and support operational activities and programs. As a result, NPPD stood up a temporary Mission Integration Cell, with representation from all NPPD subcomponents, to drive change management as well as other mission integration efforts.

The Mission Integration Cell focused on five key areas:

1. Situational awareness and operational coordination to provide a better understanding and common picture of cyber, physical, and human risks and ensure effective operational coordination across NPPD.
2. Coordinated collaboration with stakeholders and capacity building to strengthen the security and resilience of critical infrastructure to cyber, physical, and human risks.
3. Management and integration of NPPD's data to enable programs to utilize the data to which NPPD has access to identify trends and inform critical infrastructure security and resilience efforts for both strategic and operational purposes.
4. Coordinating NPPD's field forces to provide them with strategic management, realize efficiencies, and improve the delivery of services to public and private sector customers in the field, and addressing regional and sector priorities.
5. Establishing new business support models with a focus on providing better customer service from NPPD business support functions and ensuring program offices have the support necessary to be agile and dynamic in achieving NPPD's operational mission.

By focusing on these areas, NPPD will address current organizational challenges, foster a healthier, more functional organization, and ensure that NPPD has the ability to anticipate and react to evolving threats and hazards.

The Mission Integration Cell stood up working groups to gain the perspective of the workforce in developing recommendations, including interim and long-term solutions. Working groups met throughout the summer and fall of 2014 and delivered recommendations for leadership consideration.

Over the winter, a team of NPPD and DHS headquarters staff reviewed NPPD core functions with the objective of determining next steps to establish NPPD as an operational component within the Department. Based on outcomes of the core functions review, working group recommendations, and the broader work of the Mission Integration Cell, NPPD has taken action to implement interim solutions and has

developed a plan for comprehensive organizational change in support of NPPD becoming an operational component.

Interim Solutions

Based on the recommendations of working groups on situational awareness and operational coordination and customer engagement, two leads were appointed to serve in a temporary capacity to initiate proposals for NPPD leadership based on the recommendations and to explore potential process, policy, and organizational improvements. The Integration Director for Customer Engagement has established a Customer Engagement Steering Committee and is working with NPPD program offices to align similar customer engagement functions better and to develop a cohesive strategy for engagement as discussed in Section III of this report. The Integration Director for Operational Coordination has developed an interim solution to enhance NPPD's situational awareness capability and will facilitate the integration of the relevant activities of NPPD's operational centers. Together, the integration leads have established a Regional Integration Pilot, as recommended jointly by the two working groups, to assess an approach to integrate activities of NPPD staff located in the field and to enhance NPPD's field presence.

The Data Integration Working Group has provided recommendations that will enable integrating data and data-producing capabilities that provide a holistic view of risk to critical infrastructure assets. To support NPPD's efforts to advance situational awareness and operational coordination and customer engagement efforts, NPPD is appointing a lead for Data Integration.

Finally, to address the business support element of the Mission Integration Cell work, NPPD appointed a Director of Management in December 2014 to explore innovative solutions to improving our business support and to assess the potential adoption of alternate business support models. A study was conducted on several areas of NPPD's business support and the Director of Management is using those results to make interim and long-term adjustments. The Director of Management also has established a Management Forum to increase visibility, transparency, and dialogue between the lines of business and their customers, the NPPD program offices. Ensuring effective business support will continue to be critical to NPPD's ability to enhance operations.

Notional Organizational Structure

Based on the work conducted through the Mission Integration Cell and related assessments, DHS has determined that some realignment is called for to ensure that the organization can carry out its mission effectively in the future as an operational component and appropriately respond to evolving threats. This will require shifts from

NPPD's current structure to accomplish three strategic objectives focused on strengthening operational effectiveness: 1) achieve a unity of effort across the organization, 2) strengthen effective operations, and 3) ensure acquisition excellence and improved mission support. The critical areas for change are described below.

1) Advance Situational Awareness and Operational Coordination Capabilities

To prepare NPPD to move forward as an operational component, NPPD is building an integrated situational awareness and operational coordination capability to support operational requirements fully. NPPD is using the foundation and strength of the current NICC as well as other existing resources across NPPD to develop a capability that will serve four critical functions: 1) comprehensive situational awareness; 2) operational coordination of targeted crosscutting activities; 3) coordinated operational planning; and 4) executive briefing. The enhanced NICC will have a watch and operations coordination function responsible for ensuring that NPPD-wide situational awareness requirements are met and for serving as the central coordinating point for NPPD operations, regardless of whether the incident has cyber or physical implications.

2) Strengthen Cybersecurity Operations

NPPD will continue building the capability of the NCCIC and its ability to effective mitigate and respond to cyber incidents. Given the central importance of the NCCIC to the DHS mission, the NCCIC Director will report directly to the Secretary on significant incidents. In addition, NPPD will elevate the NCCIC within NPPD and add key functions of protecting the .gov domain. These organizational improvements will ensure that NPPD is positioned to meet the increasing demand for cybersecurity services across government and in support of private sector partners. The NCCIC will execute incident response operations to cyber threats for private and public sector partners, including protection of Federal networks through advanced tools that analyze data, identify trends, and respond rapidly to incidents.

3) Cohesive Approach to Stakeholder Engagement and Capacity-Building Operations

As a core part of its mission, NPPD conducts extensive engagement with government and private sector partners for the purpose of building relationships, sharing information, and assisting in capacity building. NPPD employees have spent years establishing relationships with the private and public sector, and there is an opportunity to enhance integration of programs that provide direct engagement and capacity building services as NPPD becomes an operational component. Formally aligning these programs will ensure that NPPD's partners can engage confidently on cybersecurity and infrastructure issues with the right people, and get the information they need in a timely and consistent manner. Whether engagement occurs in the field or through headquarters-based

programs, the envisioned infrastructure security function will ensure that NPPD has a cohesive approach to partnership engagement and capacity-building operations across cyber and physical risks. As NPPD moves forward with aligning customer engagement activities, consideration will be given to the unique characteristics of NPPD's programs to ensure that customer requirements are continuously met. Interim efforts through the Customer Engagement Steering Committee will ensure a smooth transition to the new structure.

4) Integrate and Enhance Regional Operations

In order to carry out NPPD's mission effectively, a robust field force is required in order to engage directly with stakeholders located throughout the Nation and to carry out NPPD operations at a local level. NPPD field forces—Protective Security Advisors, Cyber Security Advisors, Chemical Security Inspectors, Federal Protective Service officers, and Emergency Communications Coordinators—are highly respected and are a critical part of NPPD's mission, especially maintaining and sharing situational awareness and responding to incidents. To create efficiencies, improve the delivery of services to public and private sector customers in the field, and ensure that NPPD is addressing regional priorities, NPPD will integrate and support regional operations better. The NPPD Regional Integration Pilot is assessing the benefits of integrated field forces and will provide recommendations for aligning NPPD's field forces into a more cohesive organization to support NPPD as an operational component. NPPD will enhance services to customers by developing a comprehensive long-term strategy to leverage field forces better to support all NPPD mission areas, improve field engagement, provide comprehensive direct support to employees in the field, and develop career progression for field employees. This will include analysis of regional needs, recognition of unique regional requirements that should be collectively addressed by NPPD, and logistics and administrative support.

5) Leverage Integrated and Innovative Data Solutions

Through engagements with the public and private sector, NPPD develops data on cyber and physical threats, vulnerabilities, dependencies, and interdependencies through site assessments, incident reporting, and strategic and operational analysis. Most of this information is collected through voluntary partnerships and is done so based on NPPD's development of trusted relationships, expertise, and effective assessment tools. The collection and use of this information is done with an eye for protecting privacy, civil liberties, and security and law enforcement information, and for maintaining business confidentiality. Now that NPPD has established the ability to develop this information and maintain proper protections, there is an opportunity to take advantage of data aggregation to provide a more holistic picture to support risk management. As such, NPPD will implement enterprise data management processes to integrate data better across the organization to provide a comprehensive picture of risks to critical

infrastructure, underpinned by appropriate policies, practices, and technologies to present greater insight to owners and operators.

6) Coordinated Management of Large Acquisition Programs

Many of NPPD's operations are dependent on tools and large-scale acquisition programs that require focused program management to ensure that projects remain on track and meet the requirements of operators. NPPD envisions a program executive office that will develop and manage key functions of all significant acquisition programs required to deliver capabilities to support operations. In implementing a program executive office, NPPD will align with best practices from DOD, where acquisitions programs are aligned under a program executive office. This organizational change will allow operational entities to focus on day-to-day operations and incident response and to reinforce processes to pursue joint capabilities to meet similar operational needs across programs. This also will enhance NPPD's program management capabilities by building a center of excellence for acquisition professionals, which will enhance NPPD's ability to deliver effective capabilities in a cost-efficient manner.

7) Effective Operations through Customer-focused Business Support

Improving the effectiveness and efficiency of business support functions will enable the organization to focus on mission functions. As noted above, NPPD currently is taking interim steps to deliver more customer-focused business support. The new structure will include a Management function that will be a central point of accountability to ensure smooth business operations across NPPD. Establishing a Management function will improve operational efficiencies for business support tasks by eliminating multiple layers of the organization. The Management function will ensure the delivery of traditional business support functions to NPPD's programs, including accounting and finance, procurement, human resources, security, information technology systems, facilities, and property. Business support roles and responsibilities will be divided between the Management function and program offices as appropriate to ensure the efficient delivery of services. The Management function will be funded partly through a direct appropriation to management and administration activities and partly through reimbursable agreements from programs to ensure accountability. The Management function will be charged with identifying improved business models to ensure that service delivery is the top priority of NPPD.

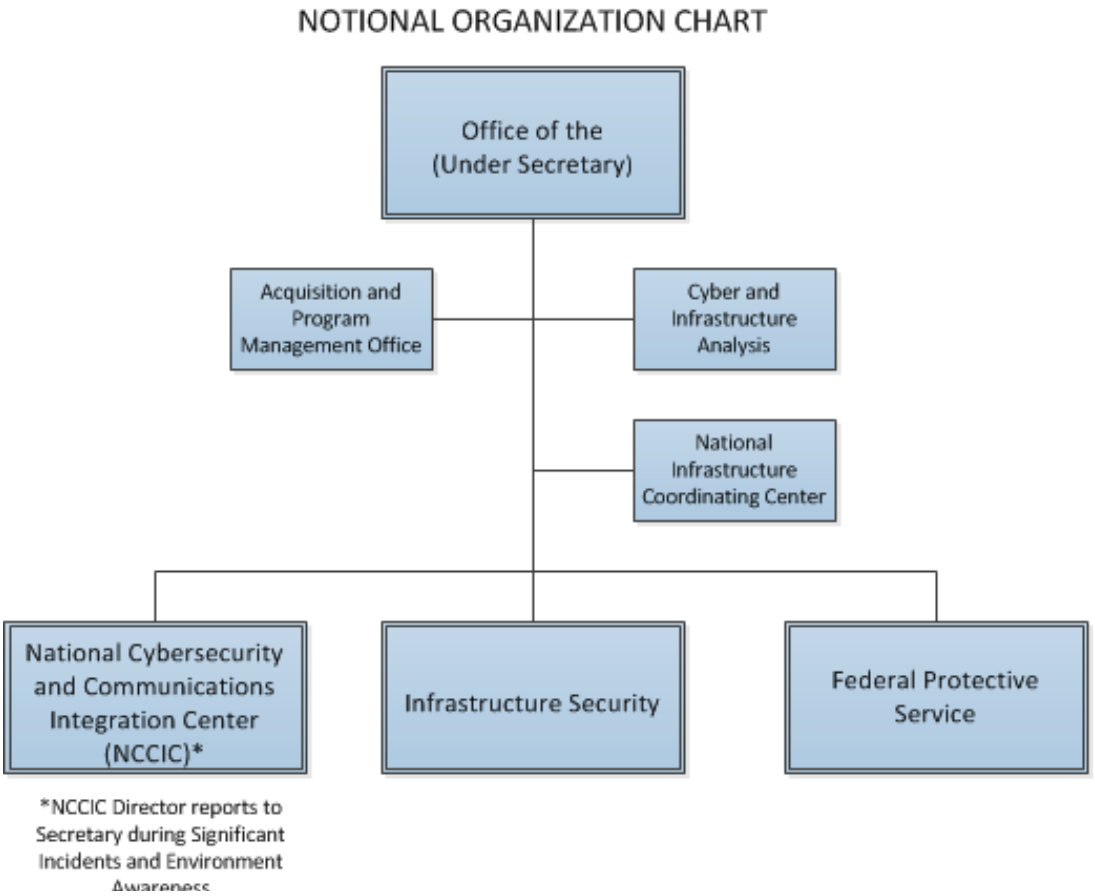
Realignment of Budget Structure to Reflect NPPD Capabilities

It should be noted that implementing the above-described activities would be facilitated by realigning its appropriations and program, project, and activity (PPA) structure consistent with the Department's Common Appropriations Structure proposal, which appropriately reflects NPPD's capabilities. The proposed appropriations and PPA

structure will enable Congress, the Office of Management and Budget, and other stakeholders to better understand what activities NPPD's funding supports and clearly tie NPPD's resources to critical infrastructure security and resilience outcomes.

Notional Organization Chart

On the basis of the critical areas of change discussed above, NPPD has a notional organization chart to serve as the framework for these changes. As NPPD continues moving forward in planning a potential restructuring, there may be additional changes to this notional structure.



VII. Conclusion

As NPPD continues to execute its critical mission, lessons learned from nearly 13 years of experience working with critical infrastructure owners and operators will be leveraged to enhance operations. NPPD's operational experience building capacity to assist the private sector and NPPD's government partners at all levels enhances security, and resilience of infrastructure will be applied more effectively across the mission space.

NPPD will continue to work in concert with its internal and external stakeholders to improve collaboration and enhance information sharing and shared situational awareness. NPPD will institutionalize and streamline its strategic and operational processes to serve its state, local, and private sector partners better as well as to deepen its understanding of risks to critical infrastructure. Similarly, NPPD will continue to build its relationships with Federal partners that it supports through both the protection of the .gov domain and Federal facilities nationwide. Continuous feedback and measurement mechanisms will enable NPPD to strengthen its partnerships, add value to its customers, and continue to evolve and adapt to the changing risk landscape.

NPPD will continue to facilitate information sharing directly through existing programs, such as the Government and Sector Coordinating Councils, Enhanced Cybersecurity Services, and CISCP, and eventually through Automated Indicator Sharing capabilities. NPPD will support private-to-private information sharing efforts by supporting the existing ISACs and encouraging the development of new ISAOs, through voluntary consensus efforts to be led by an NPPD-selected standards organization. Through these efforts, NPPD will continue to support multi-directional information between and among the public and private sectors.

NPPD also will continue to collaborate with universities, industry, and government labs to establish a large-scale test-bed to facilitate research, test new concepts, and train personnel to improve readiness and respond to natural disasters.

Finally, critical infrastructure security and resilience efforts must address all hazards - from terrorism and other criminal activities to natural disasters to cybersecurity threats. NPPD will realign its organization, programs, and capabilities in order to address the current risk landscape and plan for evolving threats. NPPD's proposed new structure will ensure effective and efficient mission operations.

Appendix

Los Alamos National Laboratory

Through the National SCADA Test-Bed (NSTB), Los Alamos is researching quantum key distribution (QKD) to exchange cryptographic keys that then are used in traditional algorithms to encrypt energy sector information, including smart grid data. In December 2012, the lab successfully demonstrated QKD on the University of Illinois test-bed in collaboration with the Cybersecurity for Energy Delivery Systems (CEDS)-funded Trustworthy Cyber Infrastructure for the Power Grid project[1].

Sandia National Laboratories

Sandia National Laboratories (SNL) is conducting research and development to address cyber-physical risk to critical infrastructure systems with deployments of physical test-beds and extensions of these via virtualized environments to support test, evaluation, training, and exercise. Physical test-beds include lab-based industrial control systems and full-scale physical plant security systems. Current research includes exploration of risk to these physical systems through nontraditional cyber means, as well as development and testing of mitigation technologies. In order to support at-scale testing and connectivity of control systems to IT systems and the wider internet, SNL's Emulytics program has supported development of virtualized environments that include end-to-end system components of the cyber system. Such an environment has been utilized for human-in-the-loop exercise and lessons learned via playback, and, with addition of appropriate fidelity in key systems, could be leveraged for system-level red teaming that cannot be conducted on the real infrastructure system as well as development and testing of mitigation technologies.

SNL has several active test environment facilities:

- Building Automation Test System – In 2014, the test system was developed to support project work for the Department of Defense. The system allows testing of real-time response of building automation systems to cyberattacks. It includes a Cisco switch, BACnet and MODBUS routers, and DSC controllers running physical processes such as HVAC, a chiller, a boiler, and lighting.
- Industrial Control System Field Device Test-Bed – The test-bed is located in the limited area of SNL. There are more than 40 field devices from multiple manufacturers connected to a physical process. Research is conducted to

[1] National SCADA Test-Bed, Laboratory-Led Projects: http://energy.gov/oe/technology-development/energy-delivery-systems-cybersecurity/national-scada-test-bed

understand cyber effects on physical processes and vulnerabilities at the physical/cyber interface.

- The Integrated Security Facility (ISF) – The ISF in Sandia's Technical Area V is a research, development, testing, and training area with a fully functional and integrated physical protection system (PPS). It is the only environment in the world that has the highest rigor nuclear security systems available for developing next-generation security systems and for training security engineers and technologists. In creating the facility, the physical security research and development (R&D) community can use the ISF to advance state-of-the-art PPS through PPS training, design, development, and testing and demonstration of next-generation technologies.

Through the NSTB[2] and its successor program CEDS, Sandia also is investigating moving target defenses to secure the energy sector better against attack by eliminating the class of adversaries that relies on known static addresses of critical infrastructure network devices. This project is reconfiguring network settings automatically and randomizing application communications dynamically to convert control systems into moving targets that proactively defend themselves against attack.

Idaho National Laboratory

Idaho National Laboratory (INL) has many resources that closely fit the concept of a National cyber-physical infrastructure test-bed. The INL maintains an 890-square mile area roughly the size of Rhode Island. A piece of this area encompasses INL's Critical Infrastructure Test Range Complex. Some key features of the INL Test-Bed include: 1) The National Electric Grid Reliability Test-Bed, which allows customers access to a utility-scale 138 kV transmission system and 13.8 kV overhead and underground distribution systems that can be customized for multiple power grid configurations. For testing purposes, portions of the grid can be isolated for conducting scalable performance, equipment, and system-type testing; 2) The National Wireless Test-Bed at the INL has 2,300 square kilometers of wireless testing range, providing a controlled, isolated radio frequency spectrum experimentation environment, with minimal interference from rural/urban areas, airports, or military test ranges; and 3) The National SCADA Test-Bed, which includes capabilities for Nuclear Nonproliferation Detection Testing, Water Test-Bed, Radiological Dispersion Devices Training, Aqueous Reprocessing, and 14 miles of railroad lines that could be repurposed as a rail test-bed. INL also operates multiple test-beds and ranges that provide demonstration space and equipment for cyber assessments, electromagnetic pulse experiments, sensor testing, explosives, and modeling and simulation.

[2] National SCADA Test Bed, Core and Frontier Research: http://energy.gov/oe/technology-development/energy-delivery-systems-cybersecurity/national-scada-test-bed

INL has test-bed resources currently available for the Department of Homeland Security (DHS):

- Wireless Test Bed – A full-scale research, development, demonstration, and scientific investigation test-bed for technologies related to all aspects of wireless communications systems. This capability enables industrial, federal, and academic researchers to address national challenges in infrastructure security, communications interoperability, spectrum utilization, and the reliability of wireless technologies. INL's isolated location paired with the Department of Energy's (DOE) significant investment in infrastructure created an ideal situation for those interested in full-scale wireless research.

- National Electric Grid Reliability Test-Bed – This test range includes a metropolitan-scale energy grid for full-scale testing of vulnerabilities, research and development concepts, and strategies for improving grid security in the bulk electric power sector. Geographically, the INL is the largest national laboratory in the DOE complex. INL's vast terrain consists of 890 square miles of desert plains. The laboratory's facilities are spread across this landscape in clusters similar to modern cities and urban environments. In between these nodes lie utility-scale infrastructure systems ranging from an independently operated and isolatable power grid to a low-interference telecommunications network.

- Other Testing Capabilities – INL also operates multiple test-beds and ranges that provide demonstration space and equipment for cyber assessments, electromagnetic pulse experiments, sensor testing, explosives, 14 miles of railroad lines, and modeling and simulation.

Through the NSTB, INL also is developing a methodology to allow energy sector stakeholders to analyze technical, cybersecurity threat information and understand how those threats affect their overall risk posture. The methodology provides a framework for analyzing technical security data and correlating that data with threat patterns, allowing stakeholders to formulate an appropriate response to a given threat.[3]

Pacific Northwest National Laboratory

Pacific Northwest National Laboratory's (PNNL) work in cyber-physical systems spans from facilitating scientific research to implementation and operations. PNNL has several research-scale test-beds to facilitate R&D. They've been sponsored through internal capability development (LDRD) funding and external projects and are used to work on problems of interest to United States Government sponsors across a broad agency set.

[3] National SCADA Test Bed, Core and Frontier Research: http://energy.gov/oe/technology-development/energy-delivery-systems-cybersecurity/national-scada-test-bed

There are many modes of operation, but the platforms are tailored to operate as user facilities. PNNL partners with academia, industry, and United States Government sponsors to develop and test new equipment, algorithms, computing infrastructure, and engineered software packages. PNNL is interested specifically in the science and engineering of complex cyber-physical systems. These test-beds are mature and interoperable, but they are not large-scale. They are composed with physical equipment and emulated physical equipment, and integrated with control and security systems.

PNNL has three research test-beds, each with unique features. They are used for research, development, testing, evaluation, and training:

- **PowerNET** – The power networking, equipment, and technology test-bed provides power system and cyber equipment in a sandbox environment where current environments can be modeled for testing and evaluation or where new architectures, algorithms, and controls can be explored and analyzed.
- **CyberNET** – The cyber networking, equipment, and technology test-bed leverages cloud platform technology modified for scientific processes and provides the ability to model realistic cyber environments including hardware, network, software, and emulated users for cyber security application study, experimentation, and prototyping.
- **RAVEN Cyber Test Range** – RAVEN allows rapid creation of configurable, blended virtual-physical systems using low-cost, commodity components and government-off-the-shelf software.

Other hybrid test-bed environments at PNNL combine physical hardware, significant software applications, simulation environments, diagnostic tools, and rapid prototyping capabilities. This hybrid environment enables the execution of an end-to-end vulnerability assessment methodology supported by multiple hardware and software diagnostic tools and development and prototyping capabilities. Together, these enable PNNL to rapidly and thoroughly assess complex, system-of-systems hardware devices and software applications for potential weaknesses that represent potential vulnerabilities. These capabilities are focused on network infrastructures and control systems ranging from critical infrastructure scale to small process control environments.

PNNL has examined the notion of a virtual large-scale test-bed in this technical area through funding provided by the DHS Science and Technology Directorate, and lessons-learned abound. While PNNL had good experience with ‘federation’ concepts and forming large collaborative teams, the logistics of multi-site research on a common test is logistically difficult due to firewalls, proximity of equipment, and other factors. What works best is to parse the research into portions where each institution can operate the whole cyber-physical system of interest. The availability of data to support research and other activities is critical. PNNL maintains repositories of data sets to enable R&D. This

is coupled to capabilities that allow effective communication and interoperability, which facilitates research in edge analytics and other emerging areas.

Through the NSTB, PNNL and project partners are developing an integrated suite of open source tools and techniques to identify compromise in the hardware, firmware, and software components of energy delivery systems both before commissioning and during period of service. The suite includes a range of stand-alone tools that can be run locally to provide hardware supply chain assurances, to large-scale high-performance computing services that can statistically analyze system-of-systems to identify potential concerns in critical infrastructure supply chains[4].

As part of its emerging capabilities, PNNL currently is constructing a System Engineering Laboratory to house PNNL electric grid research and operations work. It also will house PNNL smart buildings capabilities. This facility will be the most instrumented infrastructure on campus and could serve as an ideal medium-scale test-bed for cyber-physical research.

Argonne National Laboratory

Resiliency research is a particular strength at Argonne National Laboratory (ANL), for the grid and for the rest of the Nation's infrastructure. The grid is arguably its most important and complex infrastructure element. ANL currently is developing a concept for a national Resilient Design User Facility, which would give researchers from industry, universities, government, and national laboratories access to ANL's physical science and computing facilities to test and simulate the resiliency of key infrastructure systems. The goal is to develop new knowledge, tools, and technologies to help communities mitigate the impacts of disasters and recover more quickly.

The starting point for infrastructure resiliency analysis is always the impact of a potential disaster on the local electrical grid. Those impacts then are analyzed to understand how they will cascade out to the region and Nation, and what additional threats come into play as the impact spreads. For example, any prolonged power disruption is a danger to local economies, public health, and safety. Power disruptions can cascade quickly across interdependent infrastructures and adjacent regions, triggering disruptions in transportation services, wastewater processing, and other critical services. Although advanced control systems have improved automated outage responses, they can also expose the power grid to new cyber risks as digital components proliferate and create new points of entry.

[4] National SCADA Test Bed, Core and Frontier Research: http://energy.gov/oe/technology-development/energy-delivery-systems-cybersecurity/national-scada-test-bed

A second concept, while not new, is the Virtual Community Platform (once) which has a large untapped potential for broader national use within the preparedness and response functionality between and within the DHS National Protection and Programs Directorate, industry, universities, and government laboratories. Its future potential was only scratched during the Capstone14 New Madrid earthquake exercise by the state of Illinois and the Illinois Emergency Management Agency and a host of other state emergency management agencies, as well as infrastructure entities.

Through the NSTB, Argonne supports efforts to develop and deploy control system standards, including the International Electrotechnical Commission 61850 substation automation standard and trustworthy wireless standards through the Industrial Society of Automation working groups. Argonne applies its oil and natural gas industry subject-matter expertise in these and other NSTB efforts[5].

[5] National SCADA Test Bed, Core and Frontier Research: http://energy.gov/oe/technology-development/energy-delivery-systems-cybersecurity/national-scada-test-bed