Executive Order 13636: Improving Critical Infrastructure Cybersecurity

Cyber-Dependent Infrastructure Identification Working Group (CDIIWG)

March 11, 2013

Homeland Security

Agenda

12:30 – 1:30	(a) Overview of Executive Order 13636
	(b) Approach to Section 9: Identification of Critical Infrastructure at Greatest Risk
	(c) Sector Participation Needs
1:30 – 1:45	Break
1:45 – 2:45	Sector-by-Sector Review of Critical Infrastructure Identification Efforts *(~3-5 minutes per sector)*
2:45 – 3:20	Discussion of Criteria Options for Screening Critical Cyber Infrastructure
3:20 – 3:30	Next Steps and Adjourn

Overview of Executive Order 13636

- *Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity* was released on February 12, 2013
- Relies on public-private collaboration to improve critical infrastructure cyber posture
- Includes elements to enhance information sharing, develop a cybersecurity framework, and create a voluntary cybersecurity program
- Requires the Department of Homeland Security (DHS) to identify the "critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security"

DHS will work with CIPAC to execute Section 9 of the EO

"Within 150 days of the date of this order, the Secretary shall use a risk-based approach to identify critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security." (EO 13636, Section 9)

- Apply consistent, objective criteria
- Stakeholders include:
  - Critical Infrastructure Partnership Advisory Council (CIPAC)
  - Sector Specific Agencies (SSA)
  - Sector Coordinating Councils (SCC)
  - Government Coordinating Councils (GCC)
  - Critical infrastructure owners and operators
- The list of identified critical infrastructure will be reviewed and updated on an annual basis
- Execution of Section 9 will be led by the Cyber-Dependent Infrastructure Identification Working Group (CDIIWG)

Homeland Security

Overview of CDII Approach (1 of 2)

- Only a small subset of U.S. infrastructure will fall under the focus of the EO activity
  - Owners and operators will have the opportunity to provide relevant information
  - A review process will be established for the identification as critical infrastructure
- Focus is on critical infrastructure that could be compromised through cyber exploitation and which, if incapacitated, could result in catastrophic national, public health, or economic consequences
  - Higher standard than debilitating, which is what is used in the base definition to define critical infrastructure
  - The Secretary of DHS will provide a list of critical infrastructure most at risk in the context of a cyber incident within 150 days of EO release
  - Commercial IT products and consumer information technology services will not be directly designated under the EO as infrastructure most at risk
- All sectors will be engaged –through engagement and initial analysis it may be determined that a sector does not have any infrastructure that meets the threshold, the focus of the initial list will not be on that sector(s)

Overview of CDII Approach (2 of 2)

- Sectors with existing CI identification processes and lists should be leveraged where appropriate
- Functions-based approach to identify critical infrastructure
  - Accounts for the virtual and distributed nature of cyber infrastructure
  - Focuses on the critical activities, services, or products being produced or provided by a sector, subsector, or mode
  - Functions are identified based on the national or regional level consequences that can result from a disruption or exploitation of the infrastructure
  - Does not identify a specific organization's assets, networks, or systems; focus is on sector functions and the types of systems that support them
- Requires the application of criteria that will be used to screen the infrastructure that aligns to the critical functions
  - Consistently applied within sectors and, where possible, across sectors as well
- Stakeholder engagement will be conducted throughout this effort
  - CDIIWG will work with sectors (SSAs, SCCs, GCCs) via the CIPAC partnership framework

Key Steps and Activities

Research and Planning — Day 1-45

- DHS/NPPD conducts research to develop: a draft list of functions and an initial list of organizations that represent this critical infrastructure. These materials will be socialized in the Identification step
- DHS/NPPD develops initial list of screening criteria. This criteria will be socialized with public and private sector stakeholders

Stakeholder Recruitment — Day 15-45

- SSAs work with CDIIWG to develop recruiting list of target stakeholders
- SSAs work with SCCs and CIPAC partners to identify and recruit key stakeholders

Identification — Day 45-90

- DHS/NPPD schedule facilitated sessions and communicate logistics. DHS will also develop and distribute meeting materials for each of the identification sessions
- SSAs and sector partners will distribute meeting materials and meting notices for each of the identification sessions
- Public and private sector stakeholders attend and actively participate in each session.

Finalization — Day 90-120

- DHS/NPPD will adjudicate feedback on each of the final draft outputs
- DHS/NPPD will consolidate final draft and prepare for final approval by DHS leadership
- SSAs will provide their respective sector, subsector, or mode's infrastructure information , as appropriate, to participants for their awareness

Approval — Day 120-150

- CDIIWG deliver final draft to DHS leadership
- DHS leadership reviews and approves final output (adjudications take place during review cycles)

Homeland Security

Sector Participation Needs

- ***Successful implementation of the EO will require substantial engagement and partnership with the critical infrastructure community, especially SSA, SCC, and GCC representatives***
- DHS/NPPD will:
  - Maintain and regularly distribute a timeline of specific milestones
  - Disseminate recruitment and meeting materials to SSAs and sector members
  - Coordinate with sectors to establish the dates/times for Identification sessions
  - Work with SSAs, SCC and GCC representatives to determine each sectors' level of involvement in this activity
- SSA, SCC, and GCC representatives should work together to:
  - Determine the appropriate target participants for this effort
  - Distribute recruiting messages to sector stakeholders
  - Manage and communicate RSVPs
  - Provide information on the sectors' infrastructure identification efforts (today's focus)
  - Make recommendations on criteria for assessing dependent infrastructure

Break

Sector Efforts to Identify Cyber Infrastructure

Each sector will have approximately 3 minutes to discuss the status of any current or past efforts to identify critical infrastructure

- What has already been done in your sector to identify critical infrastructure (cyber or other)?
- What were the criteria used to assess criticality?
- How have you assessed the impacts to disruptions to your sector from cyber events?
- *NOTE: This discussion will include how other CI identification efforts, as appropriate, are leveraged or converged for this activity (e.g. DHS's National Critical Infrastructure Prioritization Program, DHS-DOD Joint Coordination Element Critical Infrastructure Dependency Prioritization Model, DHS's Critical Foreign Dependencies Initiative)*

Criteria Development Discussion: Guiding Principles

- The process for identifying cyber-dependent infrastructure will:
  - Identify sectors' cyber-dependent infrastructure
  - Characterize the relationship between physical infrastructure and cyberspace
  - Estimate the direct impact of a cyber event on an infrastructure
  - Seek to estimate, through inference or modeling, the potential for catastrophic consequences to broader social, economic, and security systems
  - Identify and define meaningful and measurable categories of impact for use as selection criteria for inclusion on the list
- The criteria for this process will allow for:
  - Comparison across infrastructure sectors
  - Identification at various levels of aggregation (region or nation)
  - Multiple paths to selection and inclusion on the list
- Stakeholder input is necessary to shape the criteria and will be sought today

Criteria Development Discussion: Assumptions and Constraints

- This infrastructure identification activity applies risk concepts but is not a risk prioritization effort
  - Cyber is a generic threat vector; no specific type of cyber threat(s) will be considered
  - Cyber-dependence and cyber-reliance imply vulnerability; specific vulnerabilities will not be evaluated
  - Potential consequences will be identified at an aggregate level (e.g., impacts of data loss, function, network or system integrity and confidentiality, and intellectual property theft will not be independently considered)
- Functional dependencies should be included in any complete analysis of potential impact

The following approaches are not mutually exclusive. They also do not represent all potential approaches that can be applied. A defensible methodology may combine principles, concepts, or factors from each or multiple of the outlined approaches

Criteria Option: Consequence-based Approach

Analysts develop estimates within categories of impact. Impact assessments are defined in like terms by category of impact (e.g., economic impact measured in USD or USD/day, public health and safety measured in casualties [fatalities + injuries])

- Advantages
  - Provides a reference point built upon quantitative evaluations, typically informed by objective information or analysis
  - Allows sectors that have already identified their critical infrastructure to potentially use their own criteria
  - Approach is consistent with other national-level prioritization methodologies
- Challenges
  - Developing consequence estimates for all identified infrastructure is typically labor-intensive
  - Limited data availability could impede meaningful quantification of potential consequence estimates

Criteria Option: Capacity-based Approach

Reports attributes of the infrastructure that imply the potential for consequences within selected categories of impact

- Advantages
  - Uses factors that are measurable and generally understood within industries and by external audiences (i.e., minimizes the credibility risks associated with new/original measurement criteria)
  - Measures criteria using readily available information; credible third-party sources could inform the analysis in a way that—if correctly applied—limits the scrutiny placed on data source(s)
- Challenges
  - Cross-sector comparative analysis is necessarily at a high level
  - Requires diligence in assessing assets of all sizes to avoid overlooking lower-capacity infrastructure that may be critical (e.g., a small sole source supplier of an intermediate product within a crowded market segment)

Criteria Option: Functions-based Approach

Qualitatively identifies the extent of potential impacts throughout the lifecycle or supporting value-added processes that most directly impact functionality

- Advantages
  - Functions are well suited for the virtual, distributed, and automated nature of cyber infrastructure and are generally well understood among owners and operators
  - Functions are defined at a level that demonstrates measurable and meaningful output
  - Approach is not heavily reliant on quantitative structured data sources
- Challenges
  - Requires greater value judgment (within and between sectors) to characterize importance of each function
  - Will likely drive the level of aggregation up to systems rather than assets
  - Heavy reliance on qualitative assessment from subject matter experts means that the results will only be as defensible as the quality and diversity of experts involved
  - Selection thresholds are very fluid, resulting in the potential for an extensive list

Immediate Next Steps

- DHS/NPPD will:
  - Use input from today's discussion to further develop the specific criteria to be used for screening infrastructure as part of the EO cyber infrastructure identification effort
  - Schedule subsequent meeting in mid-March to review the draft criteria with SSA, SCC and GCC representatives
  - Schedule follow-on meetings with SSA, SCC and/or GCC representatives if further guidance is needed on a sector-by-sector basis
  - Schedule initial identification sessions with stakeholders and send out meeting notices
- SSA, SCC and GCC representatives should work together to:
  - Review the screening criteria that DHS/NPPD provide at mid-March meeting, based on input from today's meeting, and communicate any concerns
  - Provide additional recommendations for screening criteria to CDIIWG prior to mid-March meeting, if applicable
  - Socialize screening criteria with sector stakeholders to prepare for identification sessions hosted by DHS/NPPD

Homeland Security

Cyber-Dependent Infrastructure Identification Working Group (CDIIWG)

CyberPrioritization@hq.dhs.gov

Back-up Slides

Additional Questions for Sector Discussion

- Has your sector/subsector/mode previously identified critical infrastructure (cyber or other)?
  - In what context did this identification occur, i.e. cyber, physical, or other specific kinds of threats or risks?
  - What level of infrastructure did you identify, i.e. assets, facilities, systems, etc.?
  - What criteria were used to assess criticality?
  - Is any of this infrastructure susceptible to incidents that could have effects that are regionally or nationally catastrophic?
  - Are any results from your effort sharable with audiences external to your sector? What information sharing caveats apply?

Additional Questions for Sector Discussion

- Has your sector/subsector/mode identified specific critical infrastructure owners/operators or other forms of enterprises?
  - In what context did this identification occur, i.e. cyber, physical, or other specific kinds of threats or risks?
  - What level of enterprise did you identify, i.e. companies, subsidiaries, specific offices or facilities, associations, etc.?
  - What criteria were used to assess an enterprise's criticality?
  - Roughly how many organizations were identified (or what approximate percentage of your sector does this population represent)?
  - Are any results from your effort sharable with audiences external to your sector? What information sharing caveats apply?