

UNCLASSIFIED



DHS Integrated Task Force (ITF)

Information Sharing Working Group (ISWG)

EO 13636 & PPD-21

Dissemination of Threat Reports &
System to Track Disposition

August 14, 2013
Office of Intelligence & Analysis
National Protection & Programs Directorate

UNCLASSIFIED



Scoping EO Section 4(b)

- Roles/responsibilities of Federal Departments and Agencies in the process of delivering cyber threat reporting to private sector ¹
 - Descriptive and prescriptive, capturing ongoing activity and ensuring transparency and efficiency in future processes
 - Deliverable: Shared concept of operations (CONOPs) and strategic portions in the National Infrastructure Protection Plan (NIPP) update
- Discrete set of metrics that measure disposition of all cyber threat reports shared by the Federal government with the private sector
 - Metrics such as targeted recipient entities/sectors and classification levels, as well as enable voluntary feedback regarding follow-on actions taken
 - Deliverable: Shared CONOPs regarding metrics to be tracked
- Recommend/support, initiatives that improve policies and processes
 - May include describing information flows, exercising mechanisms to release threat information, and/or improvements to collection and analysis
 - Deliverable: White Paper and in partnership with key implementation documents

¹ Cyber threat reports are products that contain information about targeted threats to specific entities.



Drivers and Lessons Learned

- Federal Departments and Agencies coalescing to improve threat information sharing internally and externally
- Mature public-private partnership compelling improved policies and processes
 - Policies and processes need to be transparent, sustained, and broadly understood by partners
 - “Do no harm” to existing trusted relationships
- Recognition of critical infrastructure owners and operators as a priority customer and non-traditional partner
 - Capturing and understanding critical infrastructure owner and operator needs
 - Holistic look at threat information, as a component of risk assessments, for effective mitigation and customer understanding
- Ensure timely and coordinated delivery of threat information to customers, at appropriate classifications, to avoid victims becoming victims
 - Threat information should ideally be actionable and predictive, informed by all data available and assessed in partnership, when possible
 - Expand good models of success in timely and effective threat information sharing

UNCLASSIFIED



Backups

UNCLASSIFIED



Two Working Groups

Info Sharing WG (ISWG)

Situational Awareness/Info Exchange (SAIE)

- EO 13636 Deliverables:

- **4(a):** DHS, DOJ, and ODNI issue instructions to ensure timely production of unclassified reports of cyber threats and increase volume, timeliness, and quality of cyber threat information to private sector

120
Days

- PPD-21 Deliverables:

- **#1:** Develop a description (e.g. wiring diagram and data matrix) of functional relationships across the Federal Government related to critical infrastructure, as well as the two national critical infrastructure centers

180
Days

- **#3:** Identify baseline data and systems requirements to enable efficient exchange of information and intelligence relevant to critical infrastructure

240
Days

- **#4:** Demonstration of near real-time situational awareness capability for critical infrastructure, with all threats/hazards approach

- **4(b):** DHS and DOJ, in coordination with ODNI, establish rapid dissemination process of cyber threat reports; track their disposition

270
Days

ISWG Deliverable: Coherent overall process for threat sharing, tested on specific sector(s)

SAIE Deliverable: Technical requirements and exercised situational awareness capability

Value: Joint effort codifies cyber and physical protection/resiliency linkages, including in NIPP