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 threat¹ reporting to private sector
 - Descriptive and prescriptive, capturing ongoing activity and ensuring transparency and efficiency in future processes
 - <u>Deliverable</u>: Shared concept of operations (CONOPs) and strategic portions in the National Infrastructure Protection Plan (NIPP) update
- Discrete set of <u>metrics that measure disposition</u> 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
 - <u>Deliverable</u>: Shared CONOPs regarding metrics to be tracked
- Recommend/support, <u>initiatives that improve policies and processes</u>
 - May include describing information flows, exercising mechanisms to release threat information, and/or improvements to collection and analysis
 - <u>Deliverable</u>: White Paper and in partnership with key implementation documents



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

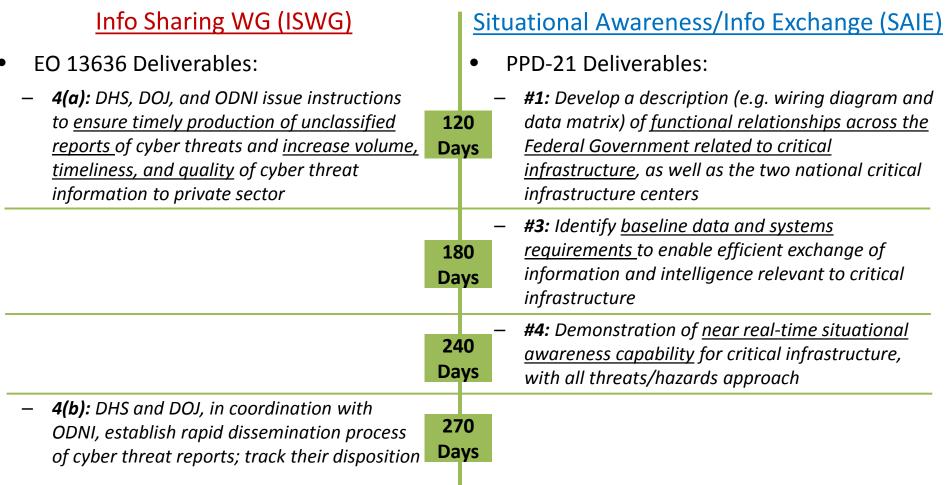
UNCLASSIFIED



Backups



Two Working Groups



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

<u>SAIE Deliverable</u>: Technical requirements and exercised situational awareness capability

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