DIB ISAC
DEFENSE INDUSTRIAL BASE
INFORMATION SHARING AND ANALYSIS CENTER

The Role of the ISACs in Critical Infrastructure Resilience

Presented by

Steve Lines
Executive Director
Defense Industrial Base Information Sharing Analysis Center
DIB ISAC

December 18, 2014

DIB ISAC
DEFENSE INDUSTRIAL BASE
INFORMATION SHARING AND ANALYSIS CENTER

Why ISACs?

- Trusted entities established by CI/KR owners and operators.
- Comprehensive sector analysis aggregation/ anonymization
- Reach-within their sectors, with other sectors, and with government to share critical information.
- All-hazards approach
- Threat level determination for sector
- Operational-timely accurate actionable

DIB ISAC
DEFENSE INDUSTRIAL BASE
INFORMATION SHARING AND ANALYSIS CENTER

ISACS

- Communications ISAC
- Defense Industrial Base ISAC
- Electricity ISAC
- Emergency Management & Response ISAC
- Financial Services ISAC
- Information Technology ISAC
- Maritime ISAC
- Multi-State ISAC
- National Health ISAC
- Oil and Natural Gas ISAC (ONG)
- Over the Road & Motor Coach ISAC
- Public Transit ISAC
- Real Estate ISAC
- Research and Education ISAC
- Supply Chain ISAC
- Surface Transportation ISAC
- Water ISAC

DIB ISAC
DEFENSE INDUSTRIAL BASE
INFORMATION SHARING AND ANALYSIS CENTER

Other Operational Sectors and Upcoming ISACs

- **Automotive**
- **Aviation**
- Food & Ag
- Nuclear
- Chemical
- Critical Manufacturing

DIB ISAC
DEFENSE INDUSTRIAL BASE
INFORMATION SHARING AND ANALYSIS CENTER

DIB ISAC Mission

The DIB ISAC was created to address an all hazards approach to securing the DIB Supply Chain. Trusted and effective threat collaboration is a critical benefit of the DIB ISAC member firms. The DIB ISAC strives to provide these firms' analyst or security officers a broad, multi-sector view of emerging threats that may extend well beyond the analyst's respective organizational domain. The DIB ISAC uses a regional outreach to ensure that member companies receive actionable threat intelligence and can also share such intelligence with partner firms. The ISAC also provides assistance in responding to and recovery from manmade and natural disasters.

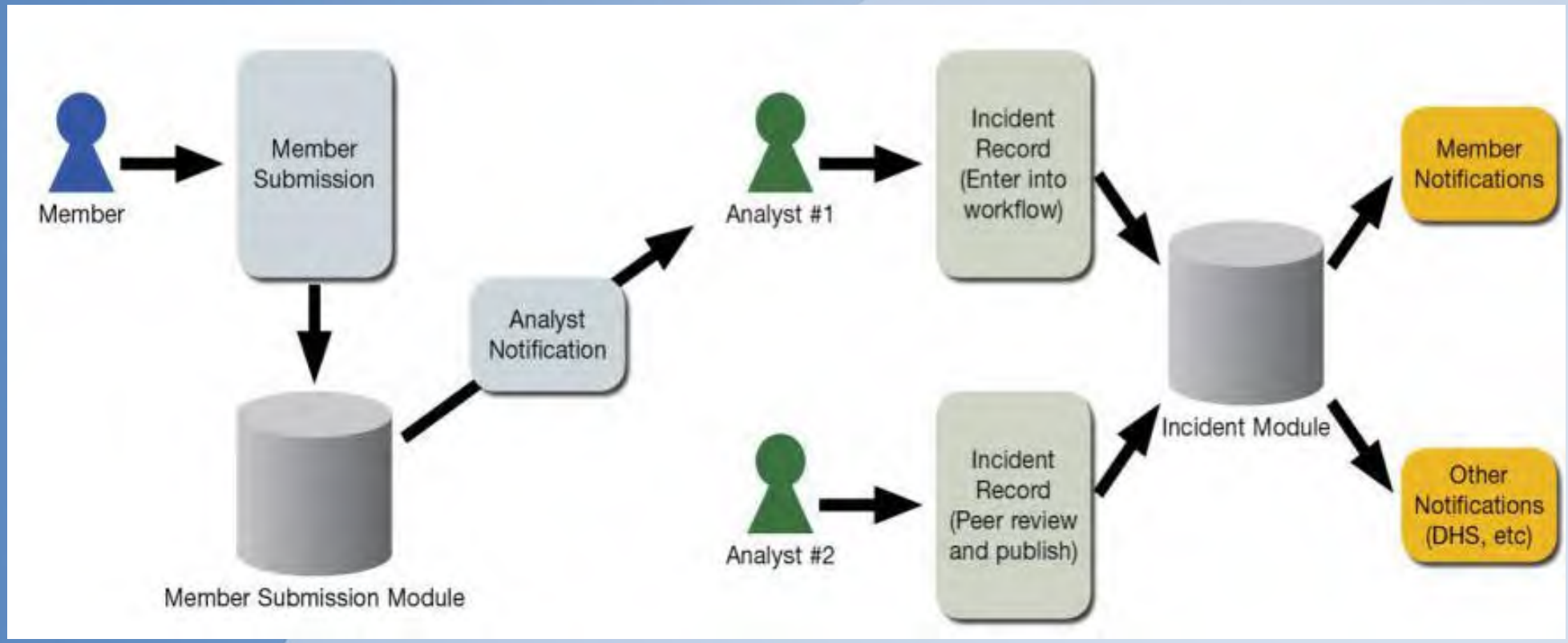
DIB ISAC
DEFENSE INDUSTRIAL BASE
INFORMATION SHARING AND ANALYSIS CENTER

Member Benefits

- Secure collaboration Platform
- Ability to share information anonymously
- Indexed threat library to share tools and techniques for securing your infrastructure
- Ability to transform threat information into a common ontology for quick analysis (STIX)
- Direct access to US Government threat products as generated by the various agencies
- Access to a community of analysts to assist in rapid analysis of threats and mitigation strategies
- Cross Sector Information sharing through the National Council of ISACs
- Access to Webcasts and other resources during nationally significant events
- Sector to sector analyst meetings and conference calls
- Community Emergency Response Training (CERT)
- Personal and Family Preparedness
- American Heart Association CPR/AED First Aid
- Continuity of Operations (COOP) support and Crisis Management

DIB ISAC
DEFENSE INDUSTRIAL BASE
INFORMATION SHARING AND ANALYSIS CENTER

Member Collaboration on a Secure Portal



Traffic Light Protocol (TLP)

- **RED** Restricted to a defined group (e.g., only those present in a meeting.) Information labeled **RED** should not be shared with anyone outside of the group
- **AMBER** information may be shared with DIB ISAC members.
- **GREEN** Information may be shared with DIB ISAC members and partners (e.g., vendors, MSSPs, customers). Information in this category is not to be shared in public forums
- **WHITE** information may be shared freely and is subject to standard copyright rules

DIB ISAC
DEFENSE INDUSTRIAL BASE
INFORMATION SHARING AND ANALYSIS CENTER

Information Sharing Flow - External

- Member RFI
  - DIB ISAC
    - Anonymizes RFI
      - NCCIC Liaison Pulls and distributes to Govt and Sector Partners
      - SITREPS on Manmade or Natural Crisis Events
      - Cyber Intel
  - Distribution Channels
      - National Council of ISACs
      - NCCIC
        - DHS Intelligence & Analysis CISCP
        - NSA NTOC
        - Federal Law Enforcement Agencies
      - UK CISP Program

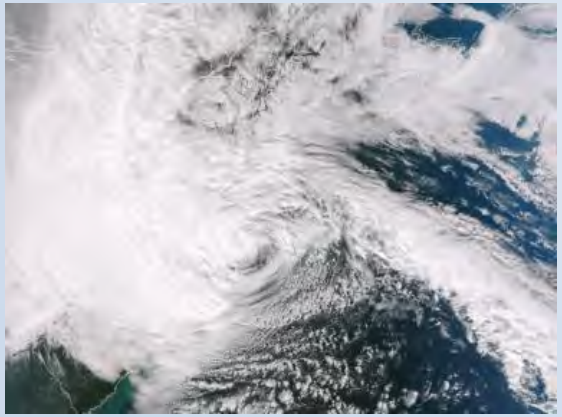
DIB ISAC
DEFENSE INDUSTRIAL BASE
INFORMATION SHARING AND ANALYSIS CENTER

National Council of ISACs

DIB ISAC
DEFENSE INDUSTRIAL BASE
INFORMATION SHARING AND ANALYSIS CENTER

Coordination During Crisis Events

- Employee Resilience and Preparedness (ERAP) custom tailored to your needs
- Corporate Emergency Response and Preparedness (CERTAP)
- American Heart Association CPR/AED First Aid
- Continuity of Operations (COOP) support
- Active support for critical infrastructure and key management relocation
- NOAA Weather Ready Nation™ Ambassador



DIB ISAC
DEFENSE INDUSTRIAL BASE
INFORMATION SHARING AND ANALYSIS CENTER

Cyber Threat Intelligence

DIB ISAC
DEFENSE INDUSTRIAL BASE
INFORMATION SHARING AND ANALYSIS CENTER

Structured Threat Information eXpression STIX

- <cybox:Observable id="fireeye:observable-1c4b8b44-10fb-4b00-8a49-deb38e92e108">
- <cybox:Title>Mutex: 8ju6thdgf</cybox:Title>
- - <cybox:Object id="fireeye:object-363367bd-7460-49bd-9163-55378a0fa666">
- - <cybox:Properties xsi:type="MutexObj:MutexObjectType">
- <MutexObj:Name condition="Equals">8ju6thdgf</MutexObj:Name>
- </cybox:Properties>
- </cybox:Object>
- </cybox:Observable>
- - <cybox:Observable id="fireeye:observable-42f1ec7e-2a32-4ff7-84a7-fbcb6288c8c9">
- <cybox:Title>Domain: www.dhcpserver.ns01.us</cybox:Title>
- - <cybox:Object id="fireeye:object-07e2d2f3-092d-436d-bbd6-60d2bdc36d43">
- - <cybox:Properties type="FQDN" xsi:type="DomainNameObj:DomainNameObjectType">
- <DomainNameObj:Value condition="Equals">www.dhcpserver.ns01.us</DomainNameObj:Value>
- <stix:Courses_Of_Action>
- - <stix:Course_Of_Action timestamp="2014-02-20T09:00:00.000000Z" id="fireeye:courseofaction-70b3d5f6-374b-4488-8688-729b6eedac5b" xsi:type="coa:CourseOfActionType">
- <coa:Title>Analyze with FireEye Calamine Toolset</coa:Title>
- <coa:Description>Calamine is a set of free tools to help organizations detect and examine Poison Ivy infections on their systems. The package includes these components: * PIVY callback-decoding tool (ChopShop module, available here: https://github.com/fireeye/chopshop) * PIVY memory-decoding tool (PIVY PyCommand script, available here: https://github.com/fireeye/pycommands)</coa:Description>
- </stix:Course_Of_Action>
- </stix:Courses_Of_Action>

DIB ISAC
DEFENSE INDUSTRIAL BASE
INFORMATION SHARING AND ANALYSIS CENTER

What Machines See
Automated Exchange-SOLTRA (National Council)

- - <stix:TTP timestamp="**2014-02-20T09:00:00.000000Z**" id="**fireeye:ttp-aedd016d-12c0-4d6e-902e-9a1cefd3e7e6**" xsi:type="**ttp:TTPType**">
- <ttp:Title>**Victim Targeting**: th3bug</ttp:Title>
- - <ttp:Victim_Targeting>
- - <ttp:Identity id="**fireeye:ciqidentity30instance-917ed96c-05c2-4754-aed9-9123341f7cb8**" xsi:type="**stixCiqIdentity:CIQIdentity3.0InstanceType**">
- - <stixCiqIdentity:Specification>
- <xpil:OrganisationInfo xpil:IndustryType="**Healthcare Sector,Higher Education Sector**" />
- </stixCiqIdentity:Specification>
- </ttp:Identity>
- </ttp:Victim_Targeting>
- </stix:TTP>
- <stix:TTP timestamp="**2014-02-20T09:00:00.000000Z**" id="**fireeye:ttp-fb6aa549-c94a-4e45-b4fd-7e32602dad85**" xsi:type="**ttp:TTPType**">
- <ttp:Title>**Spear Phishing Attack Pattern as practiced by menupass**</ttp:Title>
- - <ttp:Behavior>
- - <ttp:Attack_Patterns>
- - <ttp:Attack_Pattern capec_id="**CAPEC-163**">
- <ttp:Description>**menuPass appears to favor spear phishing to deliver payloads to the intended targets. While the attackers behind menuPass have used other RATs in their campaign, it appears that they use PIVY as their primary persistence mechanism.**</ttp:Description>
- </ttp:Attack_Pattern>
- </ttp:Attack_Patterns>
- </ttp:Behavior

DIB ISAC
DEFENSE INDUSTRIAL BASE
INFORMATION SHARING AND ANALYSIS CENTER

Cyber Verify

- Regulatory
  - DFARS Subpart 252.204.7012
- Compliance with EO/PPD directives
- Monetary
  - Contractors do not have the funds to verify or maintain verification of compliance by small mid size firms to bid on contracts to meet the new DFAR requirements
  - AT&L cannot effectively manage a program of over 17,000 CDC nationwide, the program must be managed regionally using existing resources through the Cyber Verify program

DIB ISAC
DEFENSE INDUSTRIAL BASE
INFORMATION SHARING AND ANALYSIS CENTER

Contact Info

Steve Lines

steve.lines@dibisac.net

256-489-0550 Office

256-929-8987

www.dibisac.net

YOU have an obligation to actively participate in the protection of Critical Sector assets from hostile threats and hazards!
Leverage the ISAC communities of trust!