Welcome to the Third Public Meeting of the Information Sharing and Analysis Organization Standards Organization

May 19, 2016

ISAO
Standards Organization

Information Sharing and Analysis Organization (ISAO) Standards Organization

A secure and resilient Nation; connected, informed and empowered.

Welcome!

Dr. Heidi Graham

Senior Fellow, LMI

ISAO Standards Organization

Thank You to our Food and Beverage Sponsors

pwc

SAE INTERNATIONAL®

ISAO Standards Organization

Administrative Information

- Registration
  - Unregistered attendees please go to the Registration Desk
- Anaheim Hilton
  - Restrooms are located past The Mix, on the right
  - The Anaheim Hilton is a smoke-free environment
- Emergency Procedures
  - Exit the Avalon Room and out the front entrance to the left
- Break Schedule
  - Break scheduled for 09:20 – 09:40
  - Lunch scheduled for 11:40 – 1:00
    - Various local restaurants near the Hilton
    - Restaurants in the Hilton
      - Food Court
      - Mix Restaurant
      - Poolside Bar & Grill
      - Starbucks

Public Forum Rules

- Your input is important!
  - Constructive ideas are essential to this national dialogue
  - Respect your colleagues' opinions
  - The forum will be recorded and posted on www.ISAO.org
- Debate and Discussion Time
  - Please give your name and organization before asking a question
  - Please limit comments / questions to 1 minute
- Electronic Devices
  - Please mute cell phones and take calls outside

Thank you for contributing to this important work!

Information Sharing and Analysis Organization (ISAO) Standards Organization (SO)

OPENING REMARKS

Dr. Greg White

Executive Director, ISAO SO

ISAO Standards Organization

Welcome

- Welcome to our Third In-Person Open Public Forum
  - Thank you for your interest and for the time you are spending with us on this critical topic.
  - Thanks especially to all of those who have volunteered to be part of a working group and who have helped us with the initial drafts of the documents that have been posted.
- For those who have not been part of a working group, you may still join one if you are interested, or you may simply provide comments to the documents as desired.

Overview

- Mission and Vision
- Supporting the Emerging ISAOs
- Principles to Remember
- ISAO Ecosystem
- Information Sharing Between Various Entities
- Methods to Share
- Other Issues

Mission and Vision

ISAO Standards Organization

"The cyber threat is one of the most serious economic and national security challenges we face as a Nation."

President Barack Obama, March 2010

Mission: Improve the Nation's cybersecurity posture by identifying standards and guidelines for robust and effective information sharing [and analysis] related to cybersecurity risks/incidents and cybersecurity best practices.

Vision: A more secure and resilient Nation that is connected, informed and empowered.

Supporting the Emerging ISAOs

- SWG 5 establishing documents and processes to mentor new ISAOs
- The type of issues being raised:
  - Inquiries on how to create an ISAO and requesting guidance
  - Requests for how to receive more information on the standards that are produced
  - Requests to obtain a listing of current ISAOs
  - How are ISAOs formed
  - A desire for a resource to view current ISAO and ISAC organizations related to a specific sector or industry to consider joining and participating with
  - Are ISAOs going to have to register themselves
  - How will the organizations be evaluated for applying the standards in development
  - Are there any resources for specific industries to find and evaluate current and newly formed ISAOs
- We need to continue the creation of documents that will help answer these and other questions that are of interest to emerging ISAOs

ISAO Principles to Remember

- From EO 13691
  - ISAOs may be organized on the basis of sector, sub-sector, region, or any other affinity, including in response to particular emerging threats or vulnerabilities. ISAO membership may be drawn from the public or private sectors, or consist of a combination of public and private sector organizations. ISAOs may be formed as for-profit or nonprofit entities.
- So, ISAOs may be:
  - A Sector, sub-sector, region or any other affinity
  - Formed in response to an emerging threat or vulnerability
  - From the public or private sector or a combination of both
  - Formed as a for-profit or nonprofit entity

- So, we need to be all-inclusive: In essence, we need to allow for anybody (any group of individuals or organizations) to form an ISAO if they desire.
  - The ISAO and its members will determine what capabilities are important to them and that they want to implement.

ISAO Principles to Remember

- From EO 13691
  - The agreement … shall require that the SO engage in an open public review and comment process for the development of the standards referenced above, soliciting the viewpoints of existing entities engaged in sharing information related to cybersecurity risks and incidents, owners and operators of critical infrastructure, relevant agencies, and other public and private sector stakeholders.
- So, the documents developed will be based on:
  - An open public review and comment process
  - Solicitation of the viewpoints of existing entities engaged in information sharing
- So, we need to be engaged in an open public review and comment to obtain inputs from all who wish to participate in the development of our documents.

ISAO Principles to Remember

- From EO 13691
  - All standards shall be consistent with voluntary international standards when such international standards will advance the objectives of this order
  - The purpose of this order is to encourage the voluntary formation of such organizations

- So:
  - the standards developed will be Consistent with voluntary international standards (which we interpret to mean they will not propose mandatory requirements or regulations)
  - ISAOs will not be mandated but will be a voluntary formation of individuals or organizations

- So, a key aspect of the standards and the ISAOs is that they both will be voluntary.

ISAO Principles to Remember

- From EO 13691
  - Such information sharing must be conducted in a manner that protects the privacy and civil liberties of individuals, that preserves business confidentiality, that safeguards the information being shared, and that protects the ability of the government to detect, investigate, prevent, and respond to cyber threats

- So the process to share information should:
  - Protect privacy and civil liberties
  - Preserve business confidentiality
  - Safeguard the information
  - Protect the ability of the government to detect, investigate, prevent and respond to threats

- So, a key aspect of the standards is that the privacy and confidentiality of the information shared should be protected.

ISAO Principles to Remember

- So, in summary, some guiding principles we need to keep in mind include:
  - All-inclusive
  - Public review, comments, and development
  - Voluntary
  - Privacy and Confidentiality maintained

ISAO Ecosystem

- Need to include
  - ISACs
  - All 4 categories of ISAOs
    - Category 1: Individuals or Informal Group-Based
    - Category 2: Industry- and Sector-Based
    - Category 3: Geographically-Based
    - Category 4: Other
      - “Groups of technical individuals who have an active interest in cyber threat indicators due to their engagement of cyber defenses, or other computer technology in their business.”
  - For-profit and not-for-profit organizations that provide ISAO services-for-a-fee
  - Entities that will be willing to share with others and those that are not

Information Sharing Between Various Entities

- Members to ISAO
- ISAO to members
- ISAO to government
- Government to ISAO
- ISAO to ISAO
- Open Source to ISAO
- Citizens to/from ?

Methods to share

- Informal (phone, email, text message, etc.)
- Formal electronic mail/messages to/from individuals and organizations
- Electronic messages to/from computers (automated)

- How is this done across the entire ecosystem and how does it work when individuals or organizations can be in multiple ISAOs?

- Automated sharing will lead to data standards (STIX/TAXII or some other?)
  - Can the entire sharing/analysis/response process be automated?

Other Issues

- Analysis
  - The other half of an ISAO
  - What are the different types/levels of analysis that can occur?
  - Ultimately, who does the analysis for the entire ecosystem? Automated & Distributed?
- Trust
  - How will the amount of trust an ISAO can place on information from individuals or other ISAOs be established?
    - Not based simply on an entity being called an ISAO but rather on the capabilities/characteristics it embodies.
- Certification
  - What does “self-certified” mean?

- Global –vs– U.S.- centric

ISAO SO Key Points of Contact

- Dr. Gregory White, Executive Director, ISAO SO
- Mr. Rick Lipsey, Deputy Director, ISAO SO and Director, Stakeholder Engagement
- Mr. Brian Engle, Executive Director, R-CISC
- Mr. Larry Sjelin, Director, Standards Lifecycle Management
- Ms. Natalie Sjelin, Director, ISAO Support

- Organizational E-mail: Contact@isao.org

Information Sharing and Analysis Organization (ISAO) Standards Organization (SO)

CYBERSECURITY INFORMATION SHARING ACT 2015 UPDATE

Matthew Shabat

Strategist and Performance Manager

Office of Cybersecurity and Communications

Department of Homeland Security

ISAO Standards Organization

Homeland Security

Office of Cybersecurity & Communications

Cybersecurity Act of 2015

Title I

May 2016

Cybersecurity Act of 2015

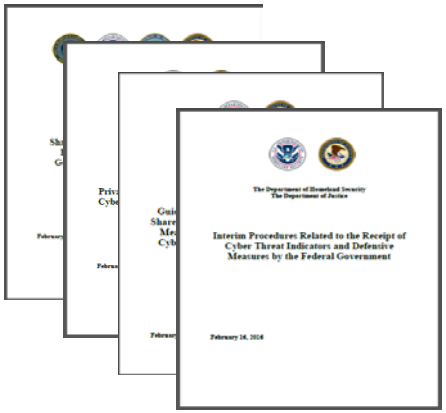
- Title 1: Cybersecurity Information Sharing Act of 2015
  - Establishes procedures, privacy protections, and liability and other legal protections
- Title 2: National Cybersecurity Advancement
  - Enhances NCCIC's intrusion detection and prevention capabilities
  - Further defines NCCIC's information sharing authorities
- Other titles cover
  - Federal cybersecurity workforce assessment
  - DHS mobile device study
  - HHS healthcare sector task force with NIST and DHS
  - Statewide Interoperability Coordinator reporting cybersecurity matters to NCCIC; NCCIC provides analysis and support

Cybersecurity Act of 2015

- Authorizes companies to share cyber threat indicators and defensive measures **with each other and with DHS**, **with liability protection**
- Identifies permitted uses of cyber threat indicators and defensive measures
- Authorizes companies to monitor their own information systems and to operate defensive measures on their systems
- Establishes privacy protections required of the sharing entity and receiving government agency

Deliverables

- Four February 16 documents (delivered to Congress and posted online):
  - Guidelines for sharing information by the Federal Government,
  - **Guidance to companies and non-federal entities for sharing cyber threat indicators and defensive measures with the Federal Government,**
  - Interim operational procedures for Federal Government receipt of cyber threat indicators and defensive measures, and
  - Privacy and civil liberties interim guidelines.



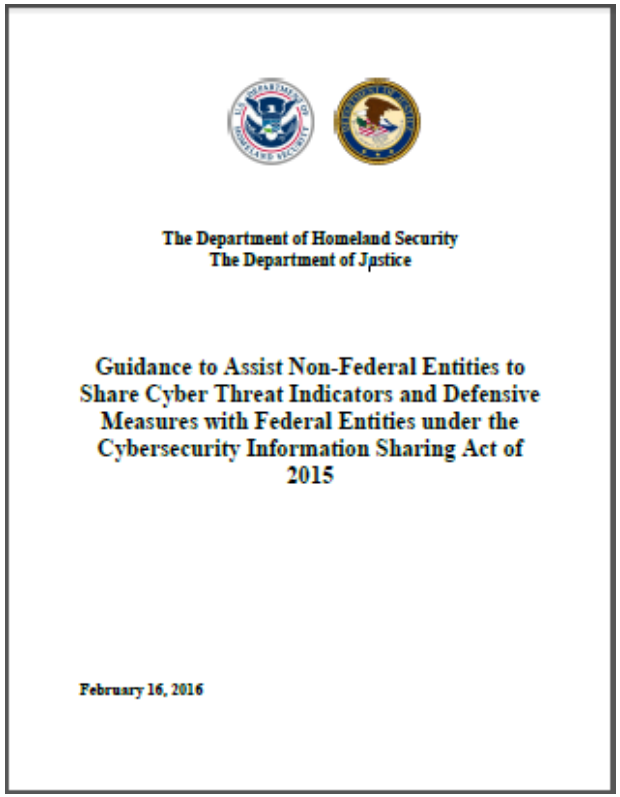
- Secretary of Homeland Security March 17 certification that automated capability authorized by Act is operational

Deliverables

- *Guidance to companies and other non-federal entities for sharing cyber threat indicators and defensive measures with the Federal Government*

  - Summary: Provides information to assist non-federal entities who voluntarily elect to share cyber threat indicators with the federal government to do so in accordance with CISA. Assists non-federal entities to identify defensive measures and explain how to share them with federal entities as provided by CISA. Describes the protections non-federal entities receive under CISA.

  - Due Date: Final at 60 days (February 16, 2016) made publicly available.



The Department of Homeland Security
The Department of Justice

Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015

February 16, 2016

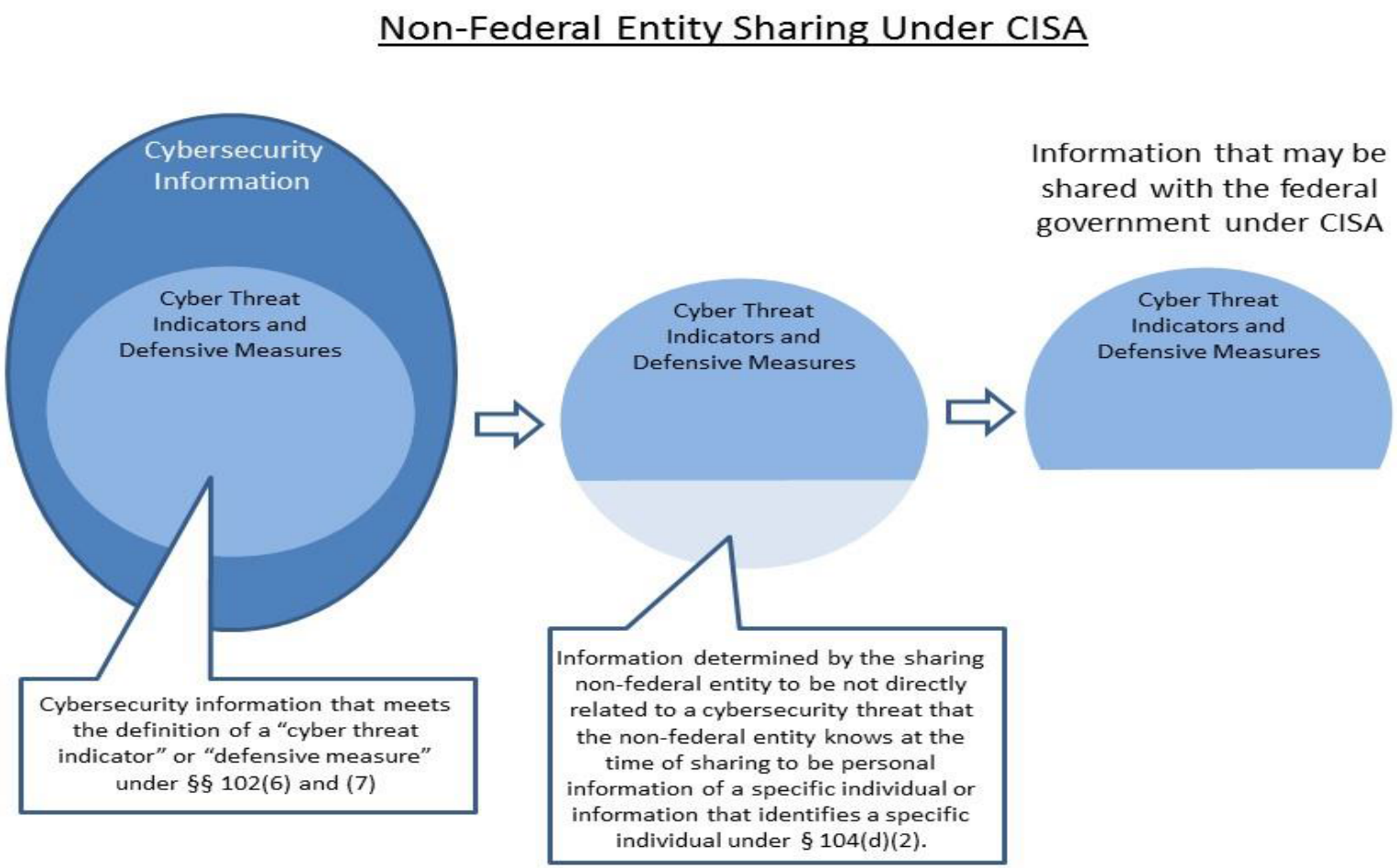
CISA Capabilities

- Automated Real-Time Capability: Automated Indicator Sharing (AIS)
  - Uses the Structured Threat Information eXpression (STIX) standard (xml format with a series of machine-readable fields) and Trusted Automated eXchange of Indication Information (TAXII) protocol

- Web Form and Email options
  - www.us-cert.gov/ais

- Privacy Scrub

Cyber Threat Indicators and Defensive Measures



Liability Protection

- The Act extends liability protection to private and other non-federal entities for sharing a cyber threat indicator or defensive measure through the Federal government's capability and process operated by DHS (automated, web form and email)
  - As long as the sharing is conducted in accordance with the Act.

- The Act also extends liability protection to sharing between and among private and other non-federal entities

- For more information please see:
  - *Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of* 2015 (available at www.us-cert.gov/ais) or
  - Section 106 of the Act.

Privacy Protections

- The Act includes various privacy protections for the receipt, retention, use and dissemination of cyber threat indicators.

- One main privacy protection requires Federal and Non-Federal entities, prior to sharing to:

  - Review such cyber threat indicator to assess whether such cyber threat indicator contains any information not directly related to a cybersecurity threat that such Federal/Non-Federal entity knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual and remove such information; or

  - Implement and utilize a technical capability configured to remove any information not directly related to a cybersecurity threat that the Federal/non-Federal entity knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual.

DHS AIS Privacy Scrub

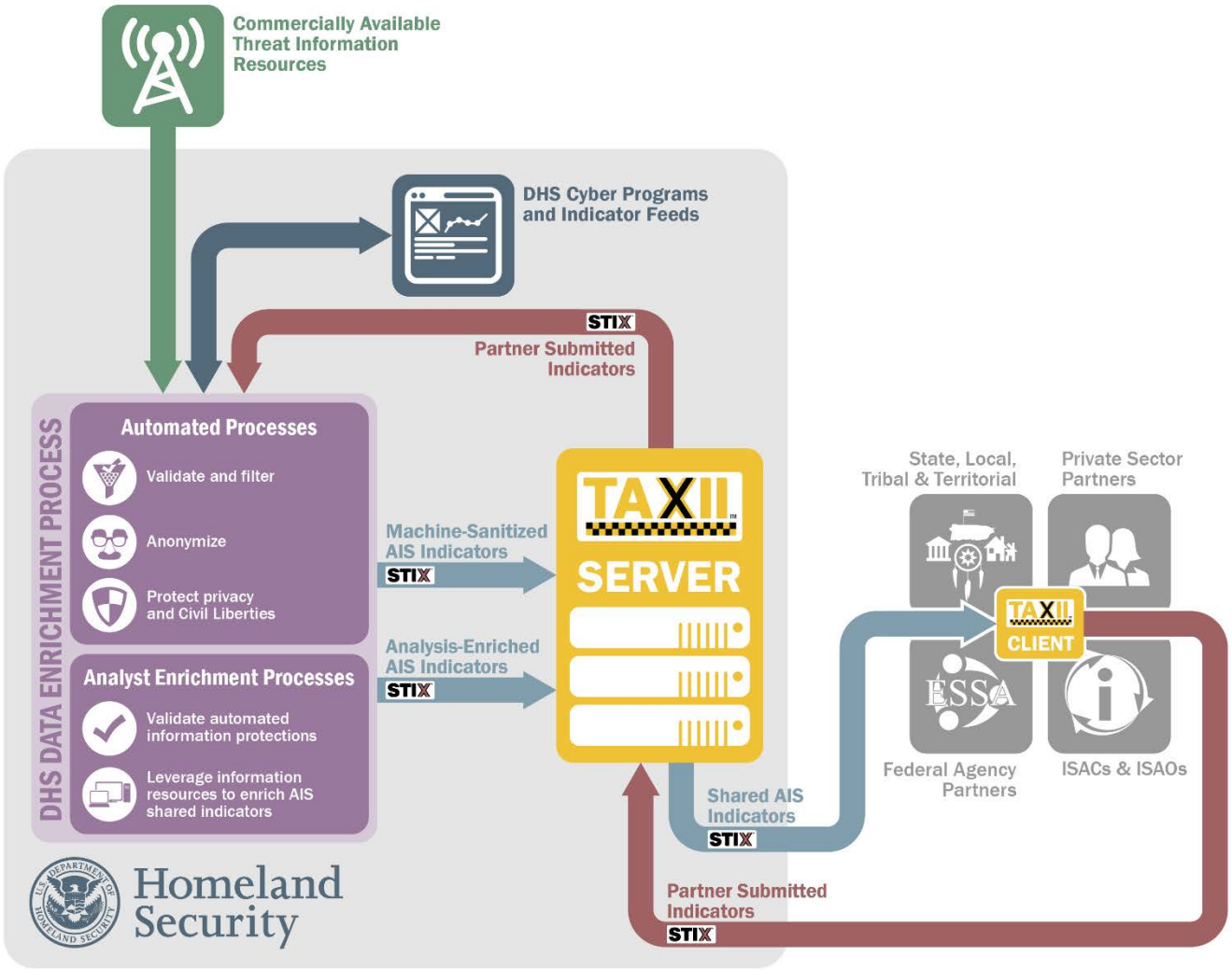
- Under AIS, DHS will receive cyber threat indicators and defensive measures through that portal in a standard, automated format and apply unanimously agreed upon controls as described in the Section 105(a)(1)-(3) procedures.

- DHS will use automated processing for mitigation of remaining personal information risks through schema restrictions, controlled vocabulary, regular expressions (i.e., pattern matching), known good values, and auto-generated text.

- Any fields that do not meet certain predetermined criteria defined through the AIS Profile and in the submission guidance will be referred for human review to ensure the field does not contain personal information of specific individuals or information that identifies specific individuals not directly related to the cybersecurity threat.

- When a field within a cyber threat indicator or defensive measure is referred for human review, DHS will still transmit the fields that do not require human review to the appropriate Federal entities without delay.

Automated Indicator Sharing



How to Sign Up for AIS

1. Sign and return the appropriate participation agreement.
   - Terms of Use (non-federal entities)
   - Multilateral Information Sharing Agreement (for Federal D/As)
2. Next, have something that can talk TAXII.
   - You can use the DHS TAXII client, an open source implementation or purchase a commercial solution.
3. Sign an Interconnection Security Agreement to document the connection and capture relevant security information.
4. Finally, we exchange certificates and you give us the IP(s) you're coming from so it can get whitelisted.



CS&C Contact Information

For more information:

- www.DHS.gov/AIS
- www.us-cert.gov/AIS

Additional Questions?

- CSCExternalAffairs@HQ.DHS.gov

Information Sharing and Analysis Organization (ISAO) Standards Organization (SO)

ENGAGEMENT BETWEEN REGULATOR FORUM AND ISAO SO

Jeffrey Goldthorp

Associate Bureau Chief

Bureau of Cybersecurity and Communications Reliability, FCC

ISAO Standards Organization

Information Sharing and Analysis Organization (ISAO) Standards Organization (SO)

INTEROPERABILITY, AUTOMATION AND SHARING AT NET SPEED

Dr. Peter Fonash

Chief Technology Officer

Office of Cybersecurity and Communications, DHS

ISAO Standards Organization

Interoperability, Automation, and Sharing at Net Speed

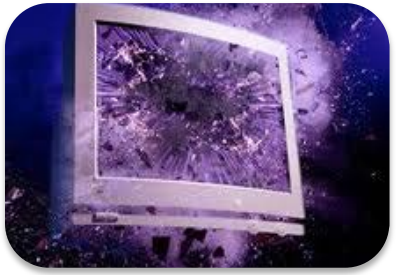
May 2016

Our Responsibilities

At CS&C, we have two complementary and related missions:

In the telecommunications arena, we support interoperability and continuity of communications needed in times of crisis.

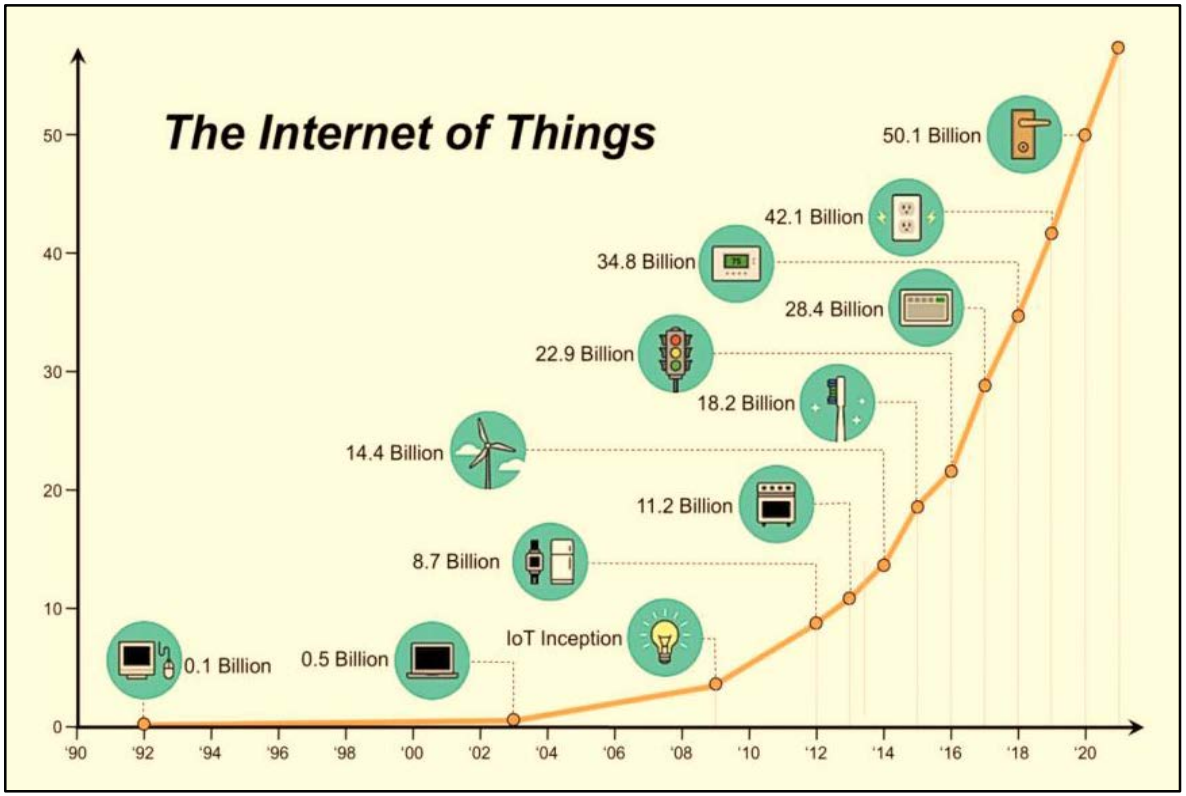
In the cyber realm, we help the ***dot gov*** and ***dot com*** domains secure themselves, focusing on critical infrastructure.



Our Challenges Grow Bigger and More Complex

We are members of a vast and expanding cyber ecosystem which consists of:

- Government and private sector information infrastructure, including international
- The interacting persons, processes, data, information and communications technologies



The cybersecurity challenge is growing every year

- The ecosystem is predicted to grow to 50B devices by 2020 [1]
- We are Increasingly reliant on cyber technologies
- The explosion in endpoints leads to an explosion in the number of opportunities for attackers

[1] D. Evans, "The Internet of Things: How the Next Evolution of the Internet Is Changing Everything," Cisco Report, April 2011

Attacks Are Continuously Expanding

Date	Company	Number of records exposed	Types of records
2/2/2015	Boston Baskin Cancer Foundation	56,694	Patient Records
2/5/2015			
2/24/2015			
2/27/2015			
3/16/2015			
3/17/2015			
5/20/2015			
5/26/2015	IRS	700,000	F
6/4/2015	OPM	21,500,000	P
7/17/2015	UCLA Health System	4,500,000	
7/19/2015	Ashley Madison	37,000,000	Finan
9/10/2015	Excellus Blue Cross Blue Shield	10,000,000	
10/1/2015	Scottrade	4,600,000	Name esses
10/1/2015	Experian	15,000,000	Personal data
11/9/2015	Comcast	590,000	email/passw ords
11/30/2015	Vtech	4,800,000 parents 6,400,000 children	Personal data
1/4/2016	Regional Income Tax Agency	50,000	
2/10/2016	IRS	101,000	Social Security Numbers
3/4/2016	21st Century Oncology	2,200,000	Patient Records

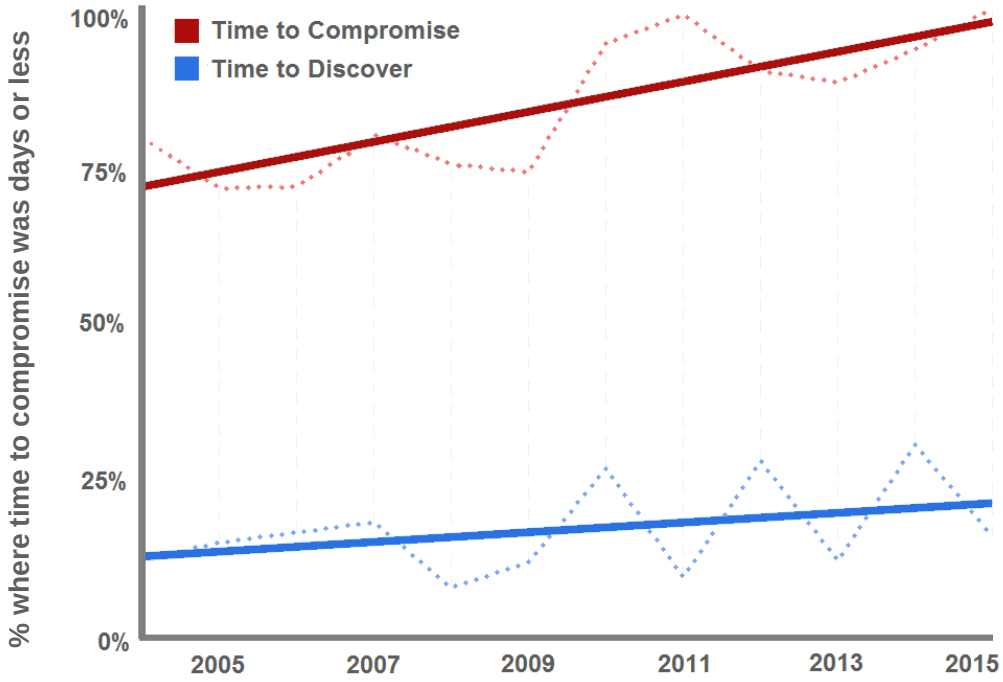
Reported June 2015:
18 Million Detailed Federal Employee Records Compromised

March 2016:
MedStar Hospitals Struck by Ransomware

- Data breach attacks continue unabated
- Greater number of individuals and organizations impacted
- Business and policy decisions are affected
- Public trust is affected

Privacy Rights Clearinghouse - http://www.privacyrights.org/data-breach
Credit Union Times - http://www.cutimes.com/2016/01/07/10-biggest-data-breaches-of-2015

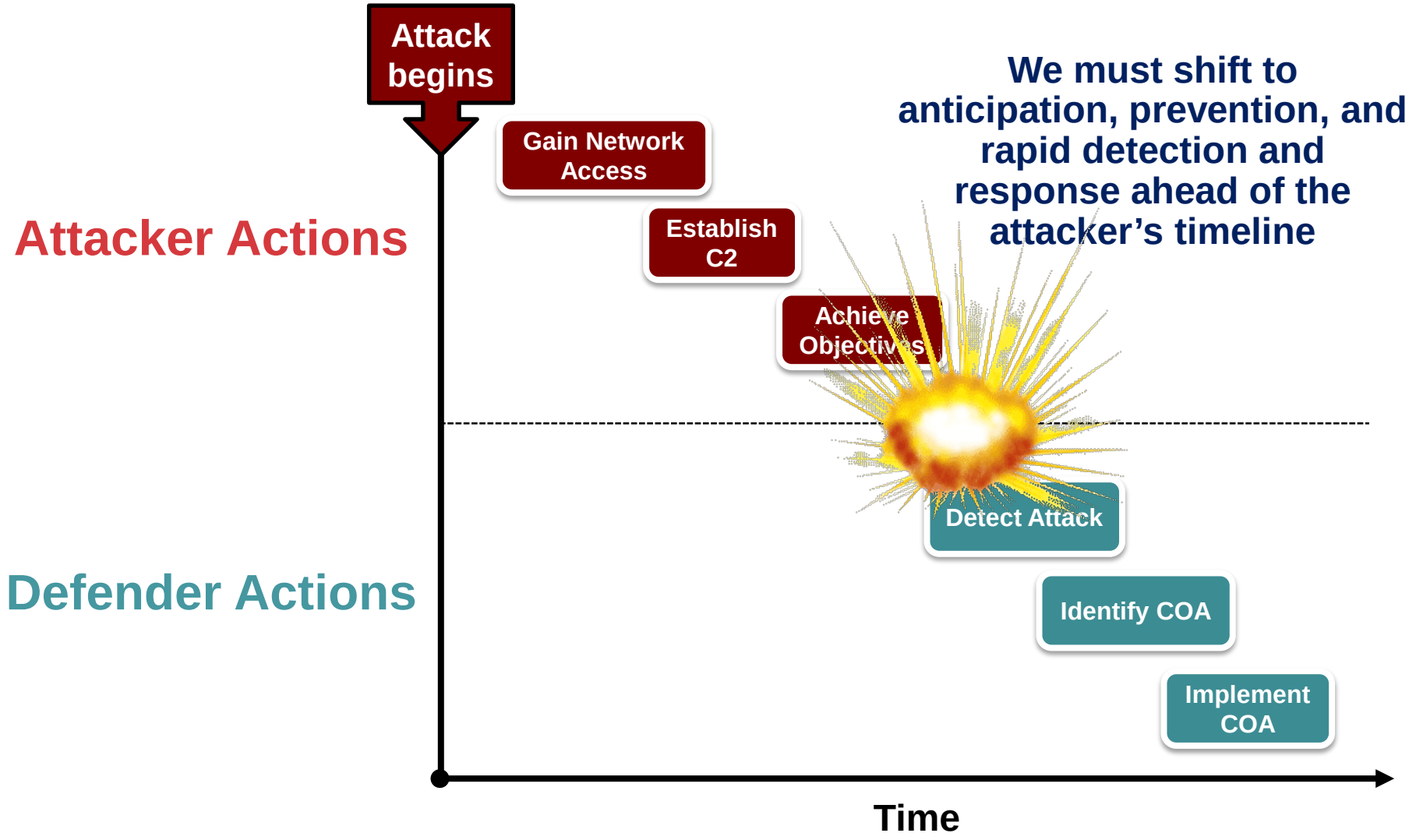
Our Opponents Improve Faster than We Do



Adapted from the 2016 Verizon Data Breach Investigations Report [3]

- Volume, sophistication of attacks go up while cost and risk to attackers decreases
- Attackers continue to improve their methods faster than defenders can adapt

Our Detection and Mitigation is Too Slow



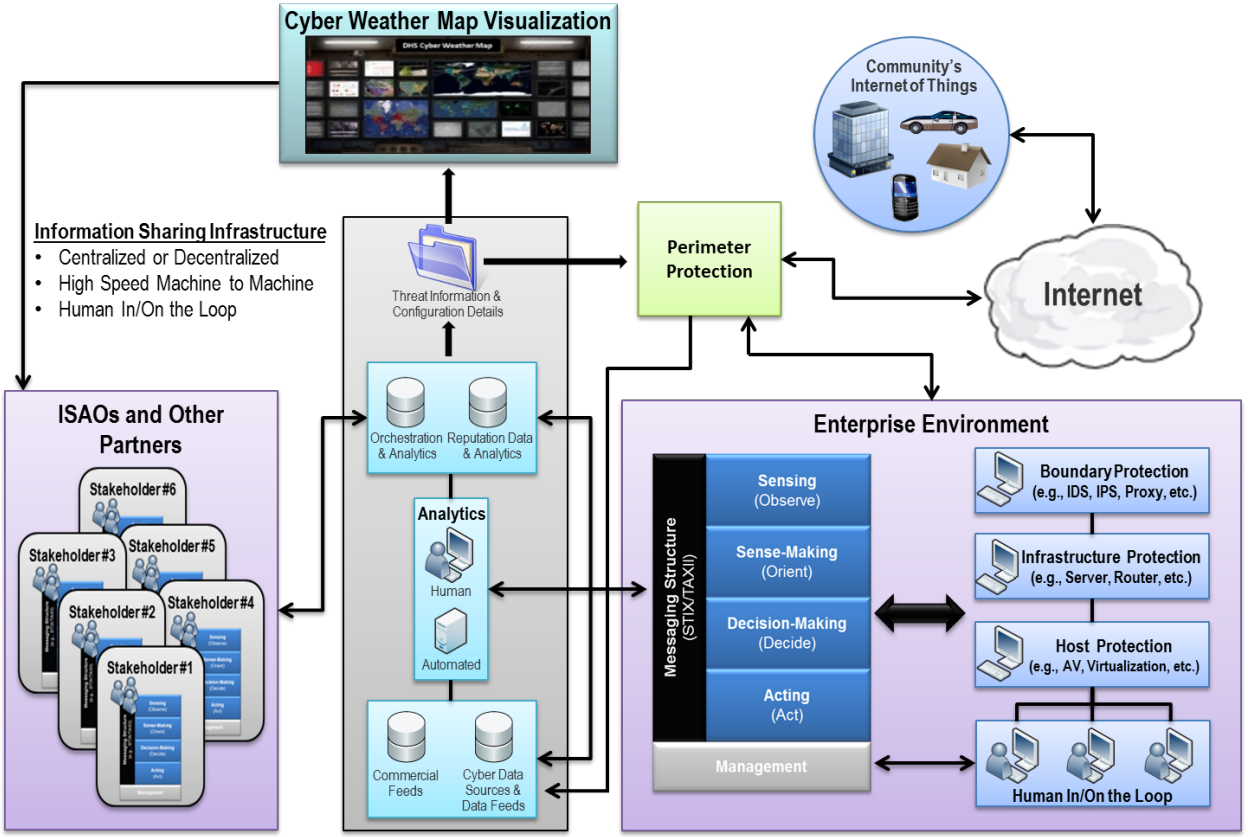
The Way Forward: Enabling Effective and Efficient Risk Mitigation

Challenges	Proposed Solutions	Mechanisms
Disparate tools don't provide integrated toolset. Costly and time consuming to integrate new innovative technology.	***INTEROPERABILITY***	Common Data Model Standards (data and transport) Open APIs, Frameworks, Control Planes Rapid Integration Acquisition
Adversaries innovating faster than defenders can adapt. IoT greatly expands the attack surface. Insufficient security analysts to meet future requirements. Defender ability to detect and respond to intrusions too slow.	***AUTOMATION***	Common Data Model Orchestration Shared COAs Security Architecture
Limited automated authentication. Lack of organizational partnerships and relationships. Insufficient trust to share and execute defensive courses of action.	***TRUST***	Authentication Infrastructure Established partnerships
Security analysts have incomplete knowledge and situational awareness of their enterprise and overall ecosystem security health. Experience of others cannot be leveraged.	***INFORMATION SHARING***	Common Data Model Information Sharing & Authentication Infrastructure
Communications infrastructure is vulnerable to attack. There is no resilient infrastructure to support assured communications.	***ASSURED COMMUNICATIONS***	Resilient Communications Priority Services Interconnected Infrastructures

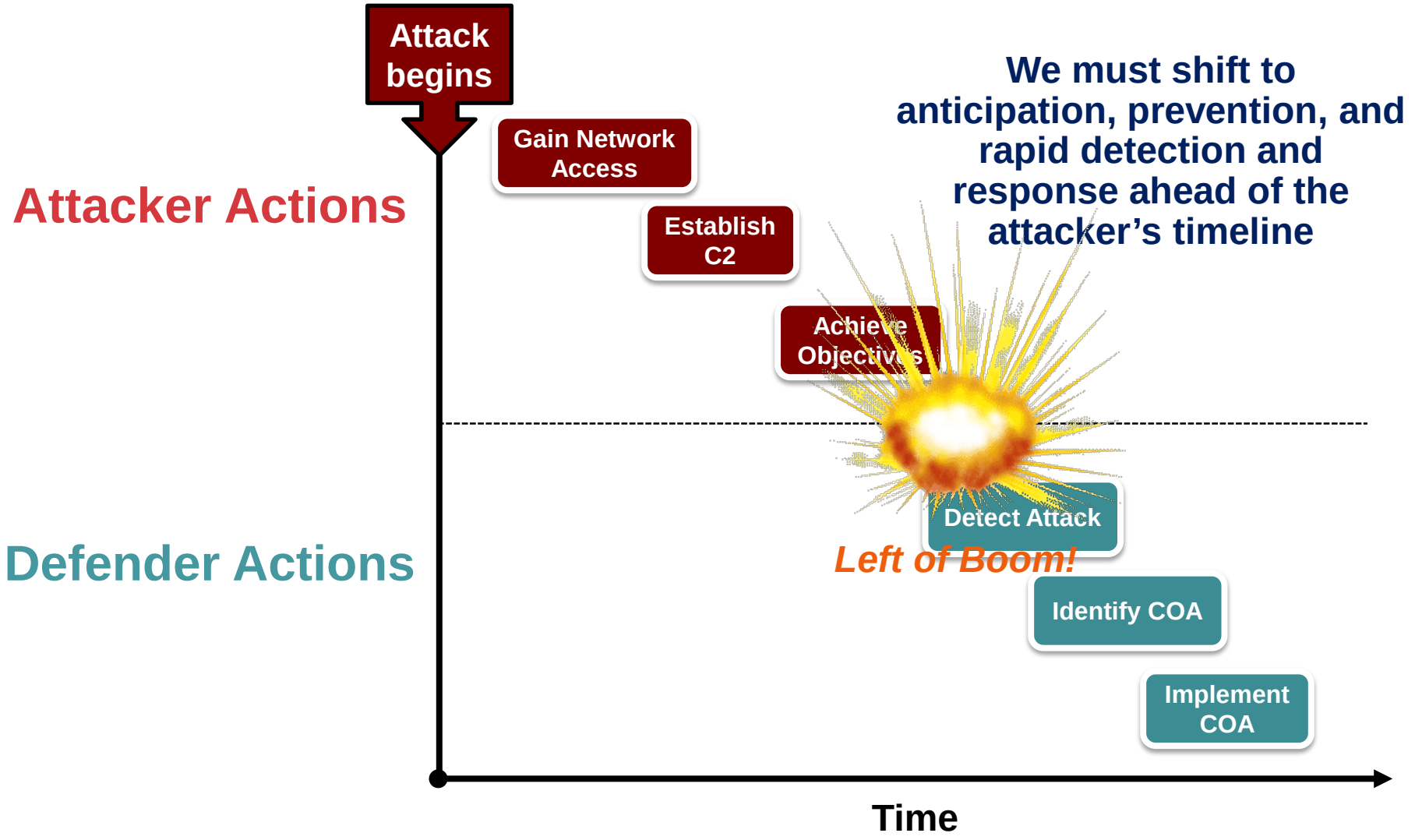
Cyber Ecosystem Example Architecture

Components

- *Enterprise Environment*
- *Cyber Weather Map*
- *Information Sharing Infrastructure*



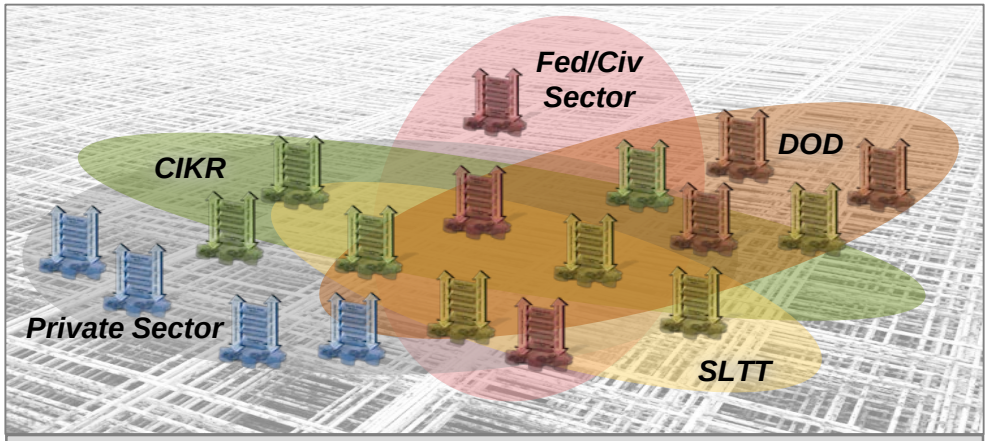
We Can Accelerate Detection and Mitigation



Where We Want to Go

Secure integration and automation across a diverse, changeable array of cyber defense capabilities

- Secure Interoperable, flexible, extensible environment available across the cyber ecosystem
- Cyber defense operations are integrated and automated according to local capabilities, authorities, and mission needs
- Proactive cyber defense has evolved from
  months ➔ minutes ➔ milliseconds
- Security operations processes and procedures are codified
- Provide operational and acquisition freedom to take advantage of diverse, changing, advanced solutions without wholesale changes to every system



Cross-Sector	Coordinate cross-sector operations and support cross-enterprise cyber response
Sectors	Enable collaborative, 'beyond-line-of-sight' defense
Enterprises	Enable participants to defend themselves

Information Sharing and Analysis Organization (ISAO) Standards Organization (SO)

BREAK

9:20 am – 9:40 am

ISAO Standards Organization

Information Sharing and Analysis Organization (ISAO) Standards Organization (SO)

PUBLIC COMMENT AND DEBATE

STANDARDS WORKING GROUP ONE: ISAO CREATION

Frank Grimmelmann, Co-Chair

Deborah Kobza, Co-Chair

ISAO Standards Organization

Information Sharing and Analysis Organization (ISAO) Standards Organization (SO)

PUBLIC COMMENT AND DEBATE

STANDARDS WORKING GROUP TWO: ISAO CAPABILITIES

Denise Anderson, Chair

Fred Hintermister, Vice-Chair

ISAO Standards Organization

Information Sharing and Analysis Organization (ISAO) Standards Organization (SO)

PUBLIC COMMENT AND DEBATE

STANDARDS WORKING GROUP THREE: INFORMATION SHARING

Kent Landfield, Chair

Michael Darling, Vice-Chair

ISAO Standards Organization

Information Sharing and Analysis Organization (ISAO) Standards Organization (SO)

LUNCH

11:40 am – 1:00 pm

ISAO Standards Organization

Information Sharing and Analysis Organization (ISAO) Standards Organization (SO)

PUBLIC COMMENT AND DEBATE

STANDARDS WORKING GROUP FOUR: PRIVACY AND SECURITY

Rick Howard, Chair

David Turetsky, Vice-Chair

ISAO Standards Organization

Information Sharing and Analysis Organization (ISAO) Standards Organization (SO)

PUBLIC COMMENT AND DEBATE

STANDARDS WORKING GROUP FIVE: ISAO SUPPORT

Carlos Kizzee, Chair

Alex Crowther, Vice-Chair

ISAO Standards Organization

Information Sharing and Analysis Organization (ISAO) Standards Organization (SO)

PUBLIC COMMENT AND DEBATE

STANDARDS WORKING GROUP SIX: GOVERNMENT RELATIONS

Michael Echols, Chair

David Weinstein, Vice-Chair

ISAO Standards Organization

Information Sharing and Analysis Organization (ISAO) Standards Organization (SO)

PUBLIC COMMENT – Q & A

Dr. Heidi Graham

ISAO Standards Organization

Information Sharing and Analysis Organization (ISAO) Standards Organization (SO)

CLOSING REMARKS

Rick Lipsey
Deputy Director, ISAO SO

ISAO Standards Organization

Thank you for attending the
Third Public Meeting of the
Information Sharing and Analysis Organization Standards Organization

Make plans now to attend the Fourth Public Meeting in Tysons, VA:

August 31st – September 1st, 2016

ISAO
Standards Organization