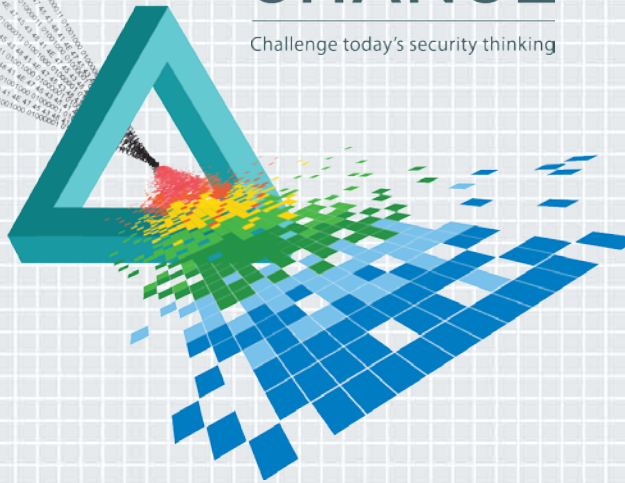
RSAConference2015

San Francisco | April 20-24 | Moscone Center

CHANGE

Challenge today's security thinking



SESSION ID: ANF-W02

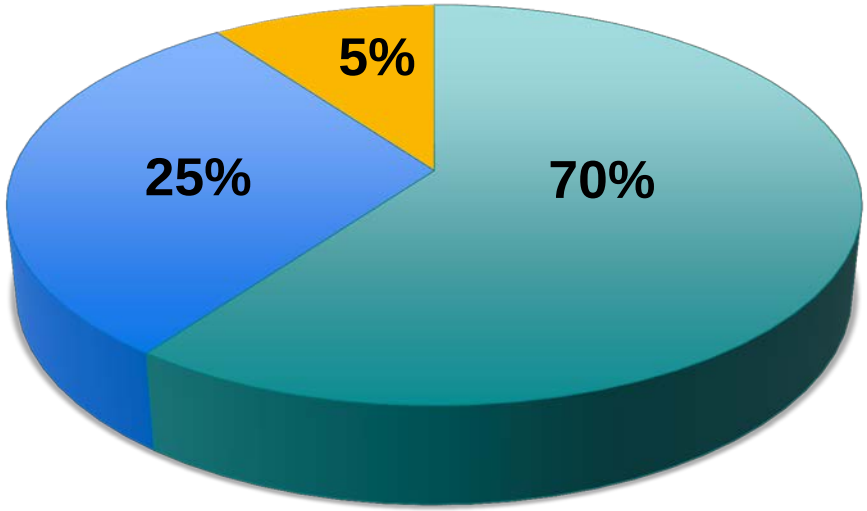
Finally We've Got Game: Real Government Info Sharing After 15 Years Of Talk

Dr. Andy Ozment

Assistant Secretary

Office of Cybersecurity & Communications, Department of Homeland Security

Cyber Risk Management



Best Practices

Cybersecurity Framework

DHS's Critical Infrastructure Cyber Community C³ Voluntary Program

Incident Response

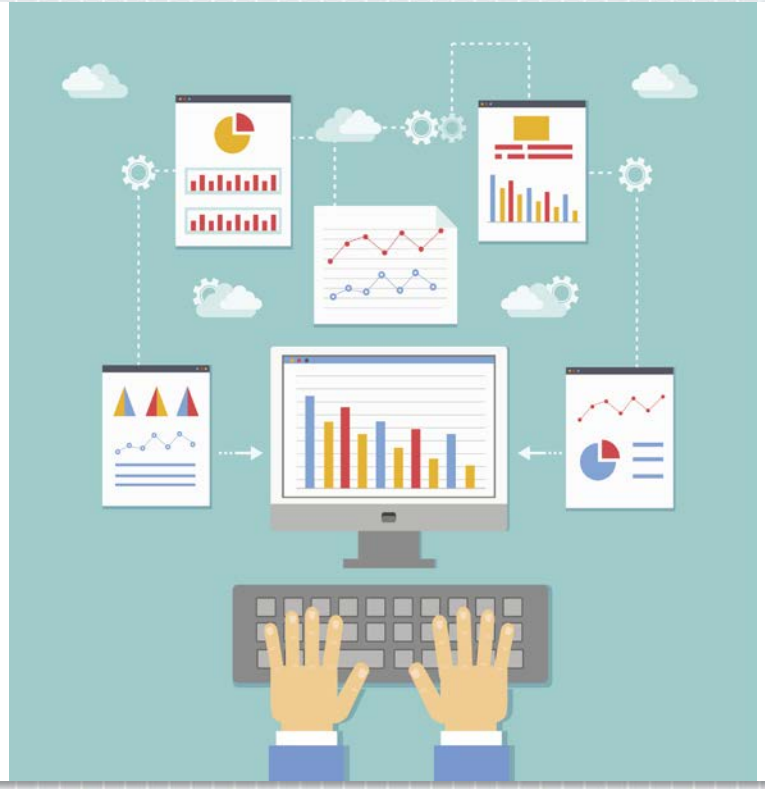
- **National Cybersecurity & Communications Integration Center (NCCIC)**: 24/7 information sharing, analysis, and incident response center
  - United States Computer Emergency Readiness Team (**US-CERT**) for information technology
  - Industrial Control Systems Cyber Emergency Response Team (**ICS-CERT**) for operational technology

Information Sharing

Federal Civilian Government

Private Sector

Big Data Analytics



Circulation

A Dream?

Government's Reality

Government's Reality

STIX/TAXII

ECS

ISAC

ISAO

CISCP

NCCIC

STIX/TAXII

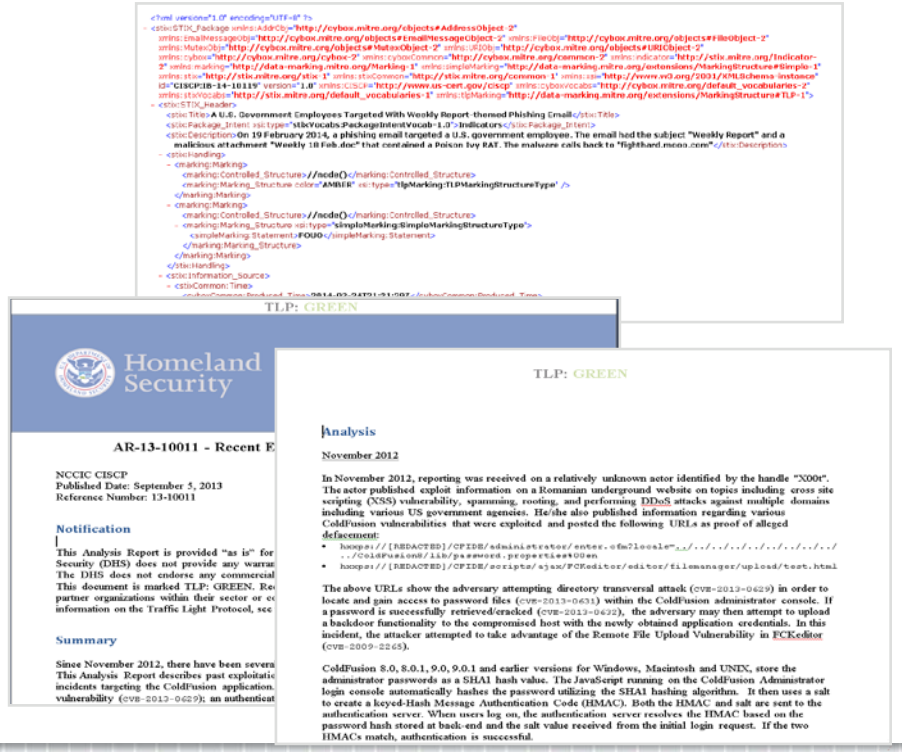

SRA
invincea
verizon
CYBERIQ
NORTHROP GRUMMAN
Goldman Sachs
tripwire
FORTINET
Booz | Allen | Hamilton
GENERAL DYNAMICS
esentire
ESSA
AMERICAN EXPRESS
CYBERSPONSE
ENABLED SECURITY
RED SKY ALLIANCE
LOOKINGGLASS
NIST
FireEye
InTELL
BY FOX IT
REVERSING LABS
Symantec.
FINANCIAL SERVICES ISAC
Microsoft
NATO OTAN
IID
splunk>
threatstream
USAA
incidentLogic
REN-ISAC
US-CERT
CENTRIPETAL NETWORKS
WORLD BANK
BLUE COAT
LOCKHEED MARTIN
HBGary
CROWDSTRIKE
CYBER THREAT ALLIANCE
hp
Palantir
DTCC
NH-ISAC
MANDIANT
fishnet SECURITY
DAMBALLA
ES ISAC
Electricity Sector Information Sharing Analysis Center
THREATCONNECT
Bromium
CERT
Cyveillance
CERT-EU
Digital Immunity
SIEMENS
FOREGROUND SECURITY
VISA
NCI Security LLC
VERISIGN
SABRE ENGINEERING
Check Point SOFTWARE TECHNOLOGIES LTD.
SOLTRA
PUNCH
ICS-ISAC
MITRE
iSIGHTPARTNERS

Live & Running

2013 **2014** **2015**

Cyber Information Sharing and Collaboration Program (CISCP)

- **Products:**
  - Indicator Bulletins
  - Analysis Reports
  - Priority Alerts
  - Recommended Practices

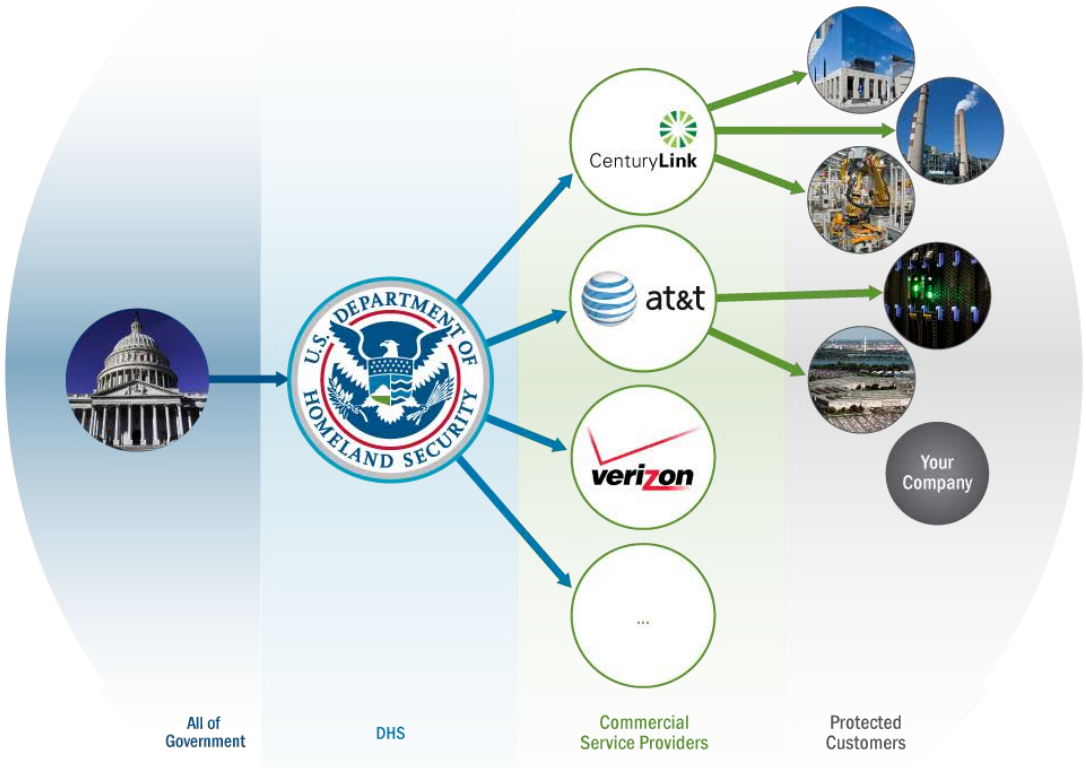


CISCP

- CISCP Analysts:
  - Share **100 threat indicators** every week
  - Have generated **1,900 products** and **30,000 threat indicators** since 2012
- **112** partner companies or ISACs
  - In discussions with **133** additional companies

Enhanced Cybersecurity Services (ECS)

Enhanced Cybersecurity Services (ECS)



NCCIC

2014:

- Received **97,000** incident reports
- Issued **12,000** actionable alerts

NCCIC/US-CERT

- Information distributed via:
  - Alerts
  - Bulletins
  - Technical Documents
  - US-CERT National Cyber Awareness System (NCAS)
  - US-CERT portal

NCCIC/ICS-CERT

- Information distributed via:
  - Alerts
  - Advisories
  - ICS-CERT Monitor
  - Joint Security Awareness Reports
  - Other Reports

ISACs


NCC


AVIATION ISAC


IT ISAC
A DECADE OF ENABLING RISK MANAGEMENT THROUGH COLLABORATION


ONG-ISAC

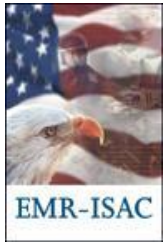

SC
ISAC


HEALTH
ISAC


ST-ISAC


REN-ISAC


APTA


EMR-ISAC


MARITIME
ISAC
MARITIME SECURITY COUNCIL
MARITIME INFORMATION SHARING & ANALYSIS CENTER


NEI


Real Estate
ISAC
Information Sharing and Analysis Center


ES-ISAC


FINANCIAL SERVICES ISAC


WaterISAC


DIB ISAC
DEFENSE INDUSTRIAL BASE
INFORMATION SHARING AND ANALYSIS CENTER

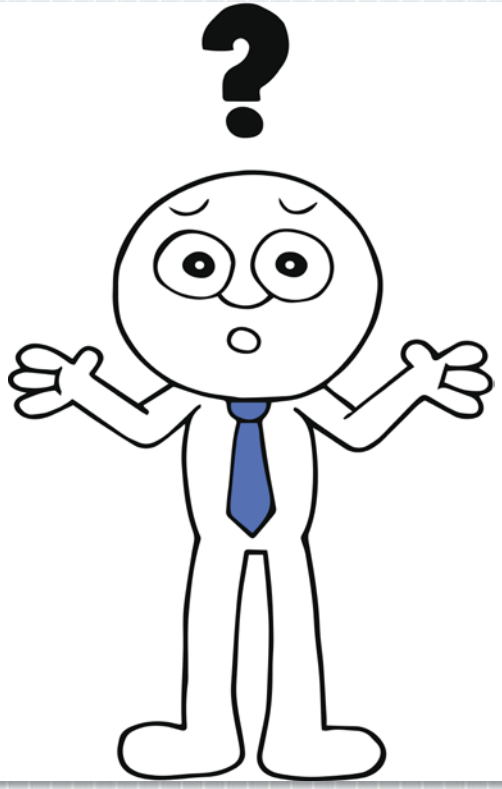

MULTI-STATE
ISAC

But…


INFORMATION SHARING AND ANALYSIS CENTERS (ISACS) OPERATE WITHIN SECTORS
Water and Wastewater Systems
Commercial Facilities
Communications
Nuclear Reactors, Materials, and Waste
Chemical
Emergency Services
Critical Manufacturing
U.S. DEPARTMENT OF HOMELAND SECURITY
Transportation Systems
Health Care and Public Health
Dams
Defense Industrial Base
Information Technology
Financial Services
Food and Agriculture
Government Facilities
Energy
16 Critical Infrastructure Sectors
= Companies
INFORMATION SHARING DATA FLOWS

Information Sharing & Analysis Organizations

But…



ISAO Best Practices

Privacy Protections

Trusted
(by individuals)

Protected Critical Infrastructure Information

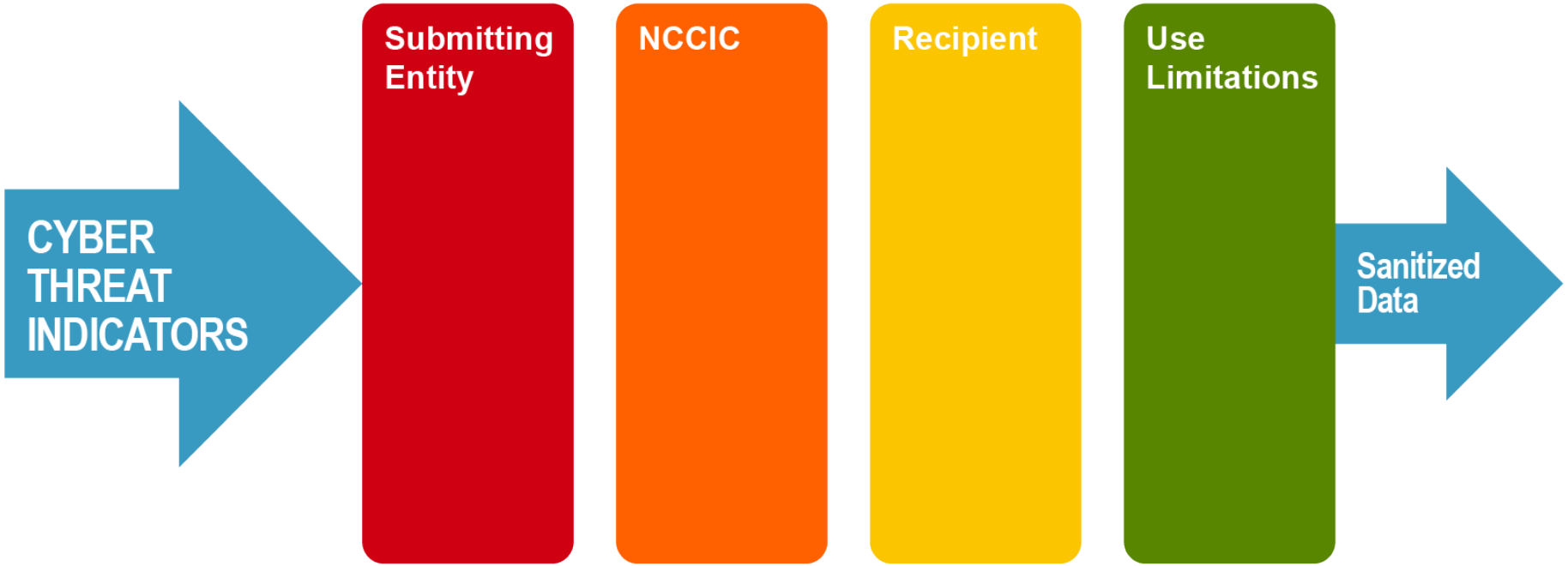
Trusted
(by companies)

Cybersecurity Legislative Proposal

Cybersecurity Legislative Proposal

- **Targeted liability protection** for companies that share cyber threat information with DHS and ISAOs
- Only **threat indicators** will be shared
- Companies will be **required to minimize personal information**
- Strong **privacy and civil liberties oversight**
- **Use restrictions**

Privacy Protections



Confused?

The Perfect Partner

- **Receives information**
  - Reports & alerts from NCCIC
  - Indicators and analyst communications via CISCP
  - Joins an ISAO to partner with peers
- **Shares information**
  - With DHS and partners via CISCP
  - With ISAO
- **Protects itself**
  - Pays Commercial Service Provider for ECS for classified intrusion prevention
  - Adopts Cybersecurity Framework
- **Responds to incidents**
  - Reports incidents to NCCIC or law enforcement
- **Builds STIX/TAXII into products**

Apply What You Have Learned Today

- Adopt the **Cybersecurity Framework**

  C³ Voluntary Program:
  www.us-cert.gov/ccubedvp

- Join **CISCP** to share with your peers & DHS

  CISCP_Coordination@hq.dhs.gov

- Subscribe to the **US-CERT National Cyber Awareness System**

  www.us-cert.gov/NCAS

- Talk to a Commercial Service Provider & pay for **ECS**

  ECS_Program@hq.dhs.gov

- Join or start an **ISAC** or **ISAO**

  ISAO@hq.dhs.gov

- Build **STIX/TAXII** into your company's products

  www.us-cert.gov/TAXII