

RSAC[®]Conference2015

San Francisco | April 20-24 | Moscone Center

SESSION ID: ANF-W02

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

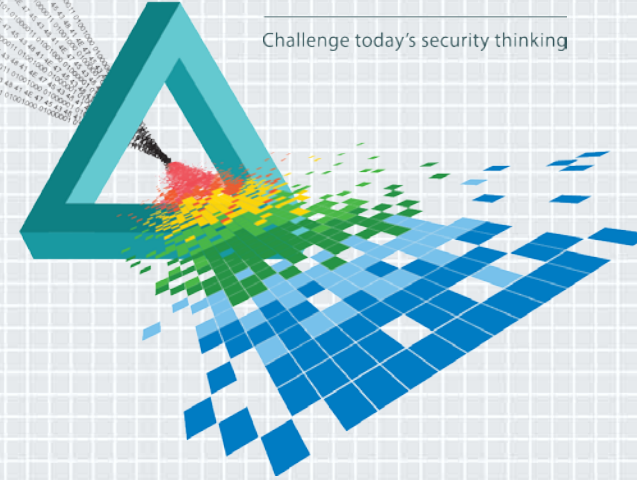
Dr. Andy Ozment

Assistant Secretary

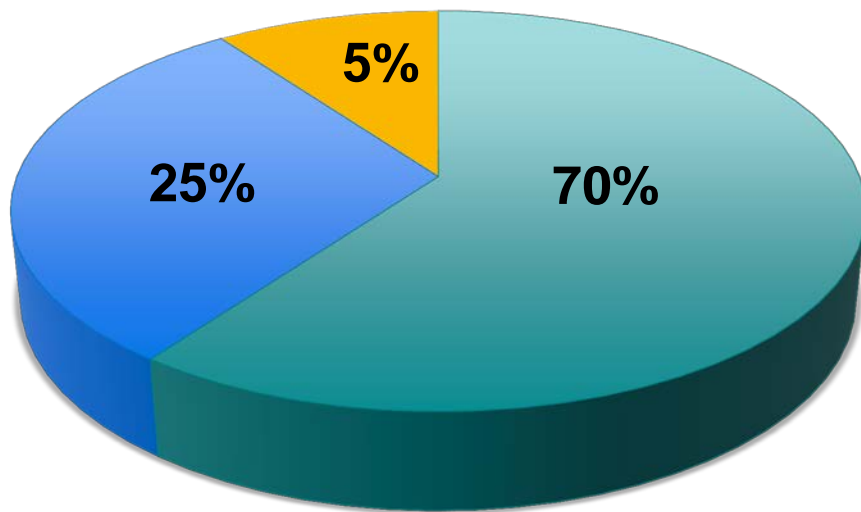
Office of Cybersecurity & Communications, Department of Homeland Security

CHANGE

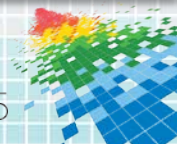
Challenge today's security thinking



Cyber Risk Management



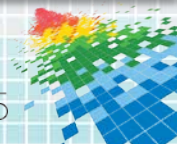
- Best Practices
- Information Sharing
- Incident Response



Best Practices

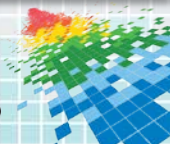
Cybersecurity Framework

DHS's Critical Infrastructure Cyber Community C³ Voluntary Program

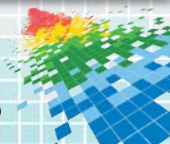


Incident Response

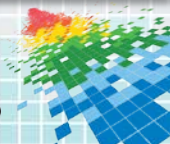
- ◆ **National Cybersecurity & Communications Integration Center (NCCIC):** 24/7 information sharing, analysis, and incident response center
 - ◆ United States Computer Emergency Readiness Team (**US-CERT**) for information technology
 - ◆ Industrial Control Systems Cyber Emergency Response Team (**ICS-CERT**)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



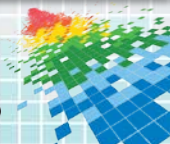
Information Sharing



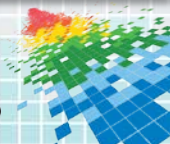
Federal Civilian Government



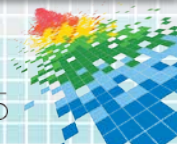
Private Sector



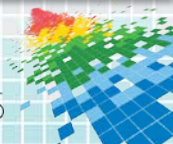
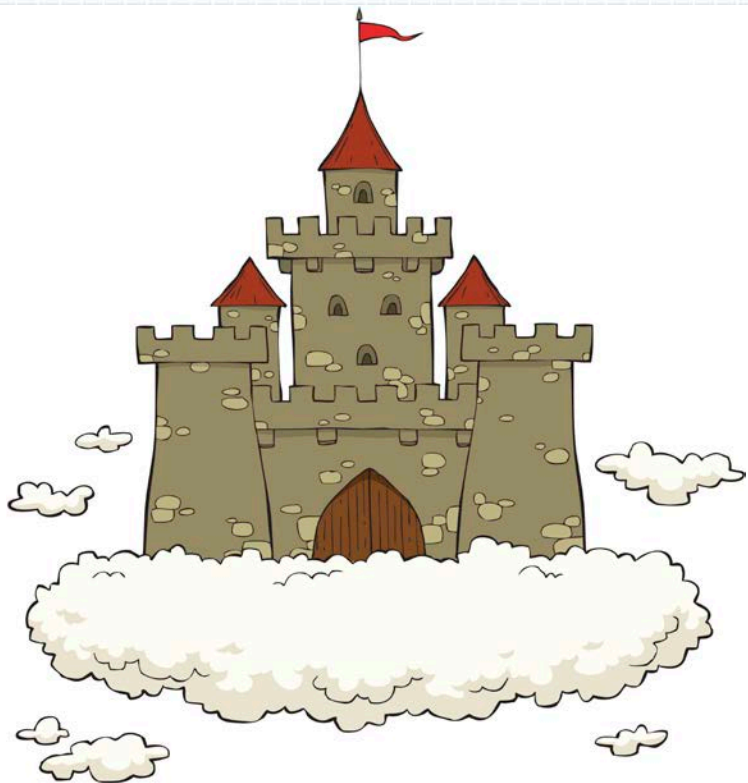
Big Data Analytics



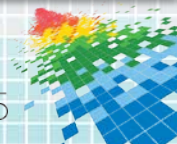
Circulation



A Dream?



Government's Reality



Government's Reality

STIX/TAXII

ECS

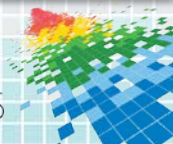
ISAC



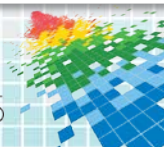
ISAO

CISCP

NCCIC



STIX/TAXII



Live & Running



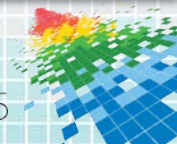
2013



2014

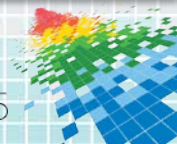


2015



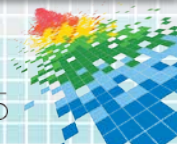
CISCP

- ◆ 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

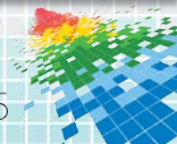


Enhanced Cybersecurity Services (ECS)

TOP SECRET



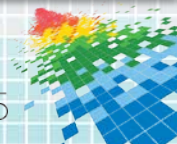
Enhanced Cybersecurity Services (ECS)



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



Official website of the Department of Homeland Security

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

HOME ABOUT US PUBLICATIONS ALERTS AND TIPS RELATED RESOURCES C'VP

US-CERT strives for a safer, stronger Internet for all Americans by responding to major incidents, analyzing threats, and exchanging critical cybersecurity information with trusted partners around the world.

Security alerts, tips, and other updates

Enter your email address

Contact Us

- (888) 282-0870
- Send us email
- Download PGP/GPG keys

Incidents, Phishing, Malware, or Vulnerabilities

Current Activity

Cisco Releases Semiannual IOS Software Security Advisory Bundled Publication

Published Thursday, March 26, 2015

Cisco has released its semiannual Cisco IOS Software Security Advisory Bundled Publication. This publication includes seven Security Advisories that address vulnerabilities in Cisco IOS Software. Exploits of these vulnerabilities could result in a denial of service (DoS) condition, interface queue wedge, or exchange memory leak.

US-CERT encourages users and administrators to review the following Cisco Security Advisory[®] and apply the necessary updates.

[Read Full Entry >](#)

Installer Hijacking Vulnerability in Android Devices

Published Tuesday, March 24, 2015

Announcements

New OMB Guidance Improves Federal Information Security

The Office of Management and Budget (OMB) established an improved process for OIG to conduct regular and proactive scans of Federal civilian agency networks. Revised Incident Notification Guidelines are included that streamline the way agencies report cybersecurity incident information to US-CERT.

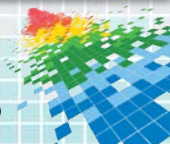
GNU Bourne-Again Shell (Bash) 'Shellshock' Vulnerability

A vulnerability in Bash, also known as 'Shellshock', affects UNIX-based operating systems such as Linux and Mac OS X. See the TA14-268A and VU#252743 for details and recommended actions.

Backoff Point-of-Sale Malware

NCCIC, USSS, and third-party partners have issued an advisory regarding a Point-of-Sale malware dubbed "Backoff" which has been discovered exploiting businesses' administrator accounts remotely and exfiltrating consumer payment data.

[More Announcements >](#)



NCCIC/ICS-CERT

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



Official website of the Department of Homeland Security

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

HOME ABOUT ICSJWG INFORMATION PRODUCTS TRAINING FAQ

Control Systems

- Home
- Calendar
- ICSJWG
- Information Products
- Training
- Recommended Practices
- Assessments
- Standards & References
- Related Sites
- FAQ

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among federal, state, local, and tribal governments and control systems owners, operators, and vendors. Additionally, ICS-CERT collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures.

Learn More about ICS-CERT

Control Systems Advisories and Reports

- Alerts**
Alerts provide timely notification to critical infrastructure owners and operators concerning threats to critical infrastructure networks.
- Advisories**
Advisories provide timely information about current security issues, vulnerabilities, and exploits.
- ICS-CERT Monitor**
We provide this newsletter as a service to personnel actively engaged in the protection of critical infrastructure assets.
- Joint Security Awareness Reports (JSARs)**
ICS-CERT coordinates with US-CERT and other partners to develop Joint Security Awareness Reports (JSARs) to provide situational awareness for the public on cybersecurity issues.
- Other Reports**
Technical Information Papers (TIPs), Annual Reports (Year in Review), and other products that ICS-CERT believes are of interest to persons engaged in protecting industrial control systems.

On This Page

- ICS-CERT Monitor Newsletters
- Recently Published
- Other Resources
- News Feed

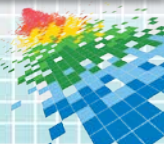
Department of Homeland Security

- Office of Cybersecurity & Communications
- Critical Infrastructure Cyber Community (C³) Voluntary Program
- NCCIC

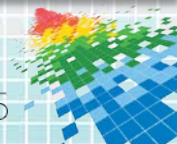
Related Resources

- Stop. Think. Connect.
- National Institute of Cybersecurity Studies
- Report Cyber Risks
- Prevent Cyber Intrusions
- Mitigate Cyber Incidents
- Cyber Resilience Review & CSET

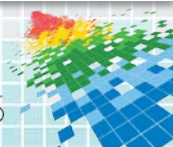
[Report an Incident](#)



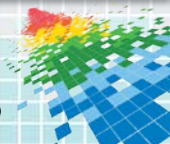
ISACs



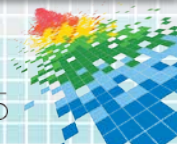
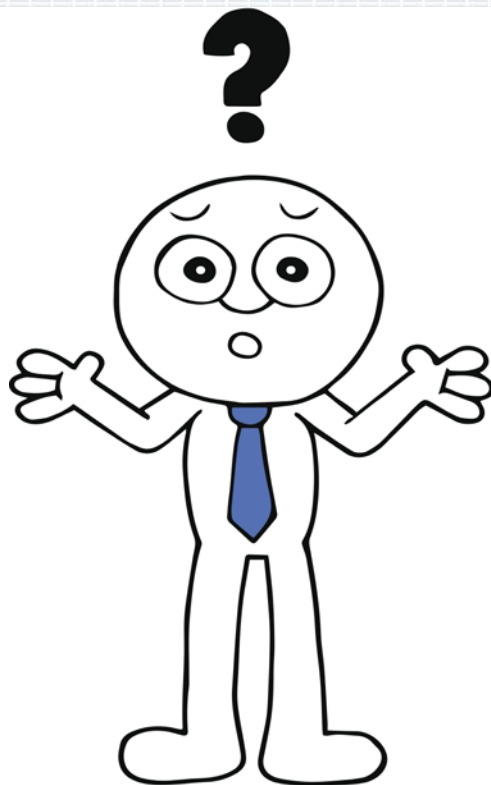
But...



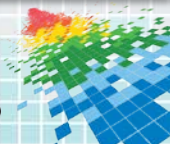
Information Sharing & Analysis Organizations



But...

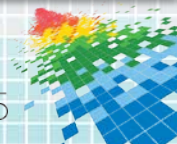


ISAO Best Practices



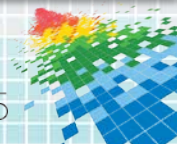
Privacy Protections

**Trusted
(by individuals)**

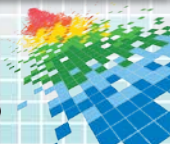


Protected Critical Infrastructure Information

**Trusted
(by companies)**

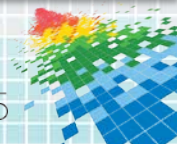


Cybersecurity Legislative Proposal

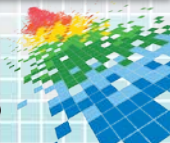
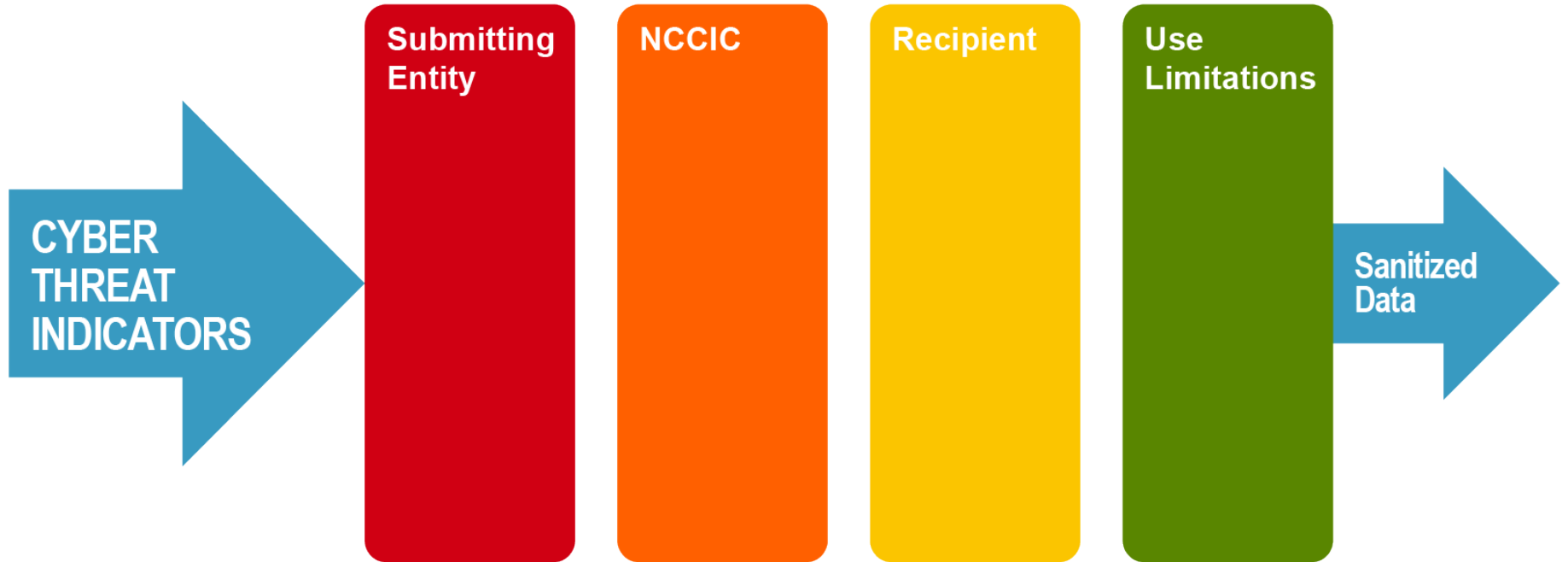


Cybersecurity Legislative Proposal

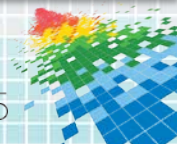
- ◆ **Targeted liability protection** for companies that share cyber threat information with DHS and ISAOs
- ◆ Only **threat indicators** will be shared
- ◆ Companies will be **required to minimize personal information**
- ◆ Strong **privacy and civil liberties oversight**
- ◆ **Use restrictions**



Privacy Protections

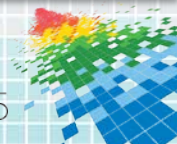


Confused?



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

