Homeland Security

2018 Legislative Ag Chairs Summit

Cyber Security

Geoff Jenista, CISSP
Cyber Security Advisor, Region VII
Office of Cybersecurity and Communications (CS&C)
National Protection and Programs Directorate (NPPD)

Cyber Security Introduction

"Cyber theft is the fastest growing crime in the United States."

- More than **six in ten** Americans own a smartphone
- Nearly **one in five** Americans has been the victim of a cybercrime
- The **weakest link** continues to be the "most valuable asset" of an organization, the **people** who sit between the seat and the keyboard
  - $2.4 million average cost of malware attack
  - 50 days to resolve insider attack
  - 23 days to resolve a ransomware attack

Critical Infrastructure


Agriculture and Food


Banking and Finance

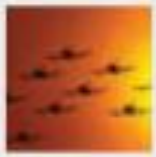

Chemical


Commercial Facilities


Communications


Critical Manufacturing


Dams


Defense Industrial Base


Emergency Services


Energy


Government Facilities


Healthcare and Public Health


Information Technology


National Monuments and Icons

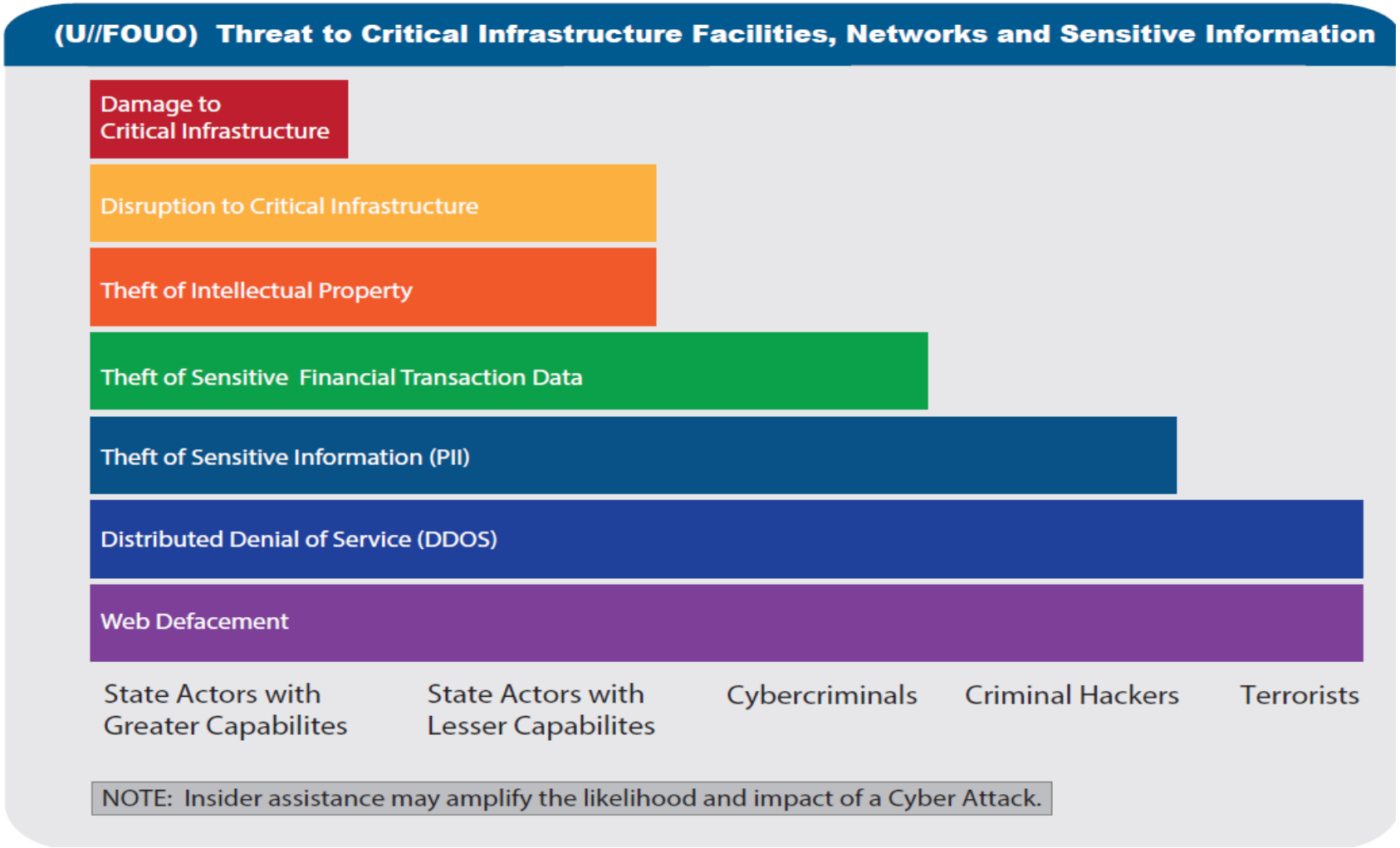

Nuclear Reactors, Materials and Waste


Postal and Shipping


Transportation Systems


Water

Threat Landscape



Cyber Security Introduction

- **Cybersecurity attacks are increasingly complex and targeted:**
  - Cyber-attacks by foreign governments threaten infrastructure, the economy, and public trust.
  - 50% of cybersecurity incidents stemmed from human error.
  - In fiscal year 2016, federal agencies reported nearly 30,899 information security incidents.
  - Cyber-crime damage costs projected to hit $6 trillion annually by 2021.
  - Cyber criminals often target smaller businesses because they tend to have fewer resources dedicated to cybersecurity.
  - A cyber incident is costly and undermines customer confidence and brand reputation.

Cyber Security General Topics

- The essential systems that support our daily are all dependent upon the Internet.
- Technology is evolving at an ever-increasing rate. Smart cities, connected devices, digitized records, as well as smart cars and homes have become a new reality.
- The Internet now touches every aspect of our daily lives, from connecting with friends on social networks to managing our finances online, but these benefits of convenience and efficiency aren't without risks.
- Every individual in an organization – from the custodian to the CEO, and the intern to the administrative assistant – has a role in cybersecurity.

Internet of Things
ShodanHQ

- ShodanHQ is the first search engine designed to search for computers and devices.
- ***Recommendation: Run a search using your network IP range to identify or validate: devices, misconfigurations, location, services, HW/SW versions, etc.***

- ShodanHQ has identified:
  - **~500,000** devices connected to the internet
  - **98,415** were located in the U.S.
  - **7,257** were associated with Industrial Control Systems

Homeland Security

Cyber Security Attacks

5 Cyber Attacks you are most likely to face:

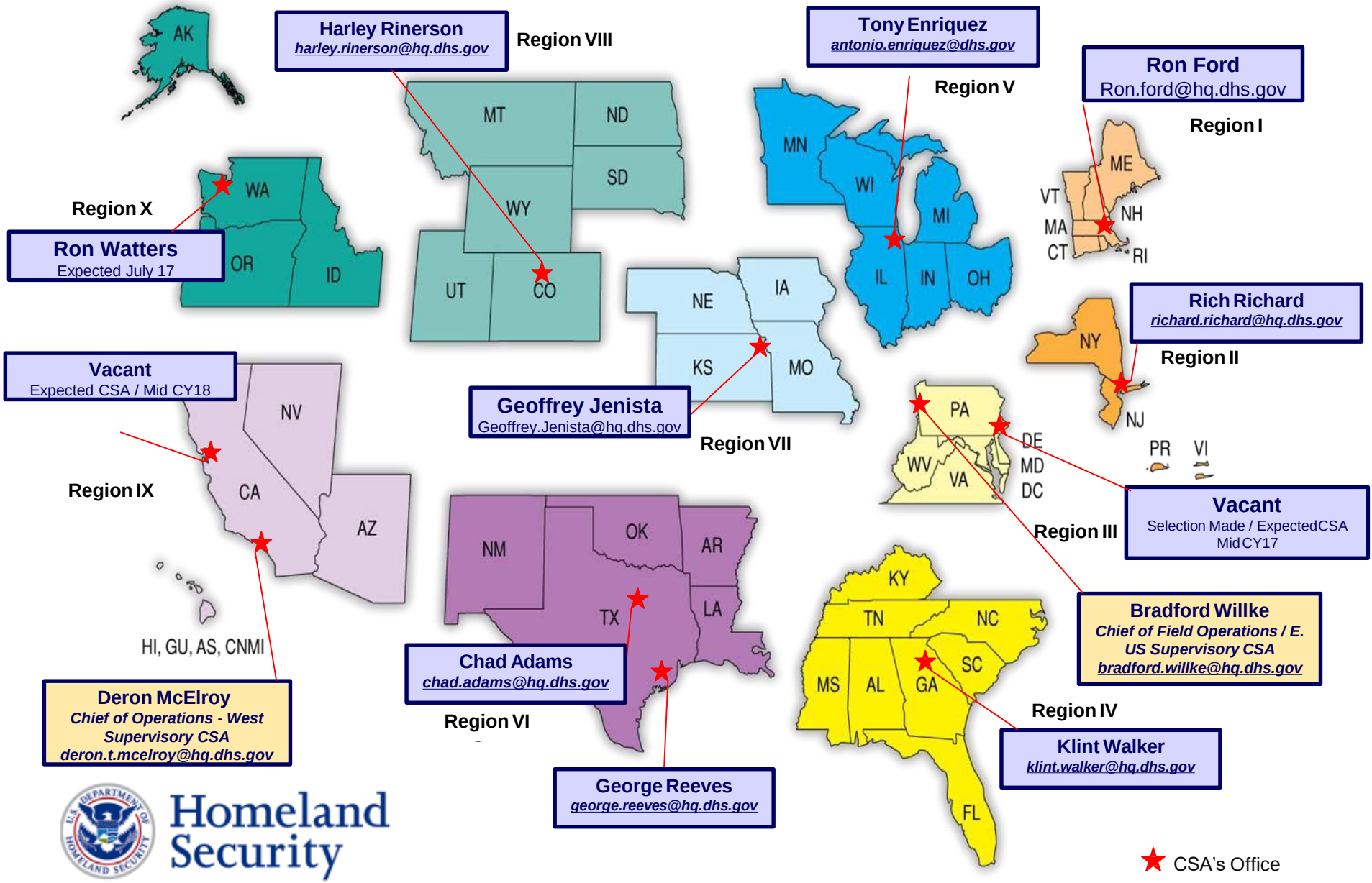
- Socially engineered malware:
  - Socially engineered malware, lately often led by data-encrypting ransomware, provides the No. 1 method of attack
- Password phishing attacks:
  - Approximately 60 to 70 percent of email is spam, and much of that is phishing attacks looking to trick users out of their logon credentials.
- Unpatched software:
  - The most common unpatched and exploited programs are browser add-in programs like Adobe Reader and other programs people often use to make surfing the web easier.

Cyber Security Attacks

5 Cyber Attacks you are most likely to face:

- Social media threats:
  - Our online world is a social world led by Facebook, Twitter, LinkedIn or their country-popular counterparts. Social media threats usually arrive as a rogue friend or application install request.
- Advanced persistent threats:
  - Attackers to send a specific phishing campaign -- known as spear phishing - to multiple employee email addresses. The phishing email contains a Trojan attachment, which at least one employee is tricked into running. After the initial execution and first computer takeover, APT attackers can compromise an entire enterprise in a matter of hours.

Cyber Security Advisors



Homeland Security

A Wide Range of Offerings for Critical Infrastructure

- National Cybersecurity and Communications Integration Center (NCCIC)
  - US-CERT Operations Center
    - Remote and On-Site Assistance
    - Malware Analysis
    - Incident Response Teams
  - ICS-CERT Operations Center
    - ICS-CERT Malware Lab
    - Cyber Security Evaluation Tool
    - Incident Response Teams
  - National Cyber Security Assessment & Technical Services (NCATS)
    - Cyber Hygiene service
    - Risk and Vulnerability Assessment
- US-CERT
  - National Cyber Awareness System
  - Vulnerability Notes Database
  - Security Publications
- Control Systems Security Program
  - Cybersecurity Training
  - Information Products and Recommended Practices
- Cyber Exercise Program
- Cyber Security Evaluations Program
  - Cyber Resilience Review
  - External Dependencies Review
  - Cyber Infrastructure Survey
- Cyber Security Advisors
- Protective Security Advisors

Contact Information

Evaluation Inquiries
cse@hq.dhs.gov

General Inquiries
cyberadvisor@hq.dhs.gov

DHS Contact Information	
Bradford Willke Program Manager, Cyber Security Advisor Program	bradford.willke@hq.dhs.gov +1 412-375-4069
Geoff Jenista Cyber Security Advisor, Region VII	geoffrey.jenista@hq.dhs.gov +1 913-249-1539

Department of Homeland Security
National Protection and Programs Directorate
Office of Cybersecurity and Communications