

# Enhancing Cybersecurity Awareness and Resiliency through Collaborative Partnerships

## ***2012 GFIRST Conference***

Critical Infrastructure Protection Cyber Security (CIP CS) Program  
National Cyber Security Division (NCSD)  
Office of Cybersecurity and Communications (CS&C)  
Department of Homeland Security (DHS)

*August 23, 2012*



**Homeland  
Security**

# Agenda

- ▶ Review cybersecurity aspects of the national critical infrastructure protection
- ▶ Describe CIP CS role in cybersecurity and critical infrastructure protection
- ▶ Discuss the importance of public-private partnerships
- ▶ Provide overview of CIP CS capabilities to increase cybersecurity awareness and sector resiliency



# The national approach to critical infrastructure and key resources (CIKR) protection is established in HSPD-7 and executed through the National Infrastructure Protection Plan

Homeland Security Presidential Directive 7 (HSPD-7)

Provides the framework and approach for the NIPP

National Infrastructure Protection Plan (NIPP)

Delineates CIKR partner authorities, roles and responsibilities

## **CIKR partners create the national approach to CIKR protection**

- Sector-Specific Agencies (SSA)
- DHS
- State, Local, Tribal, and Territorial Governments
- Private Sector Owners and Operators
- Other Stakeholders Involved with CIKR

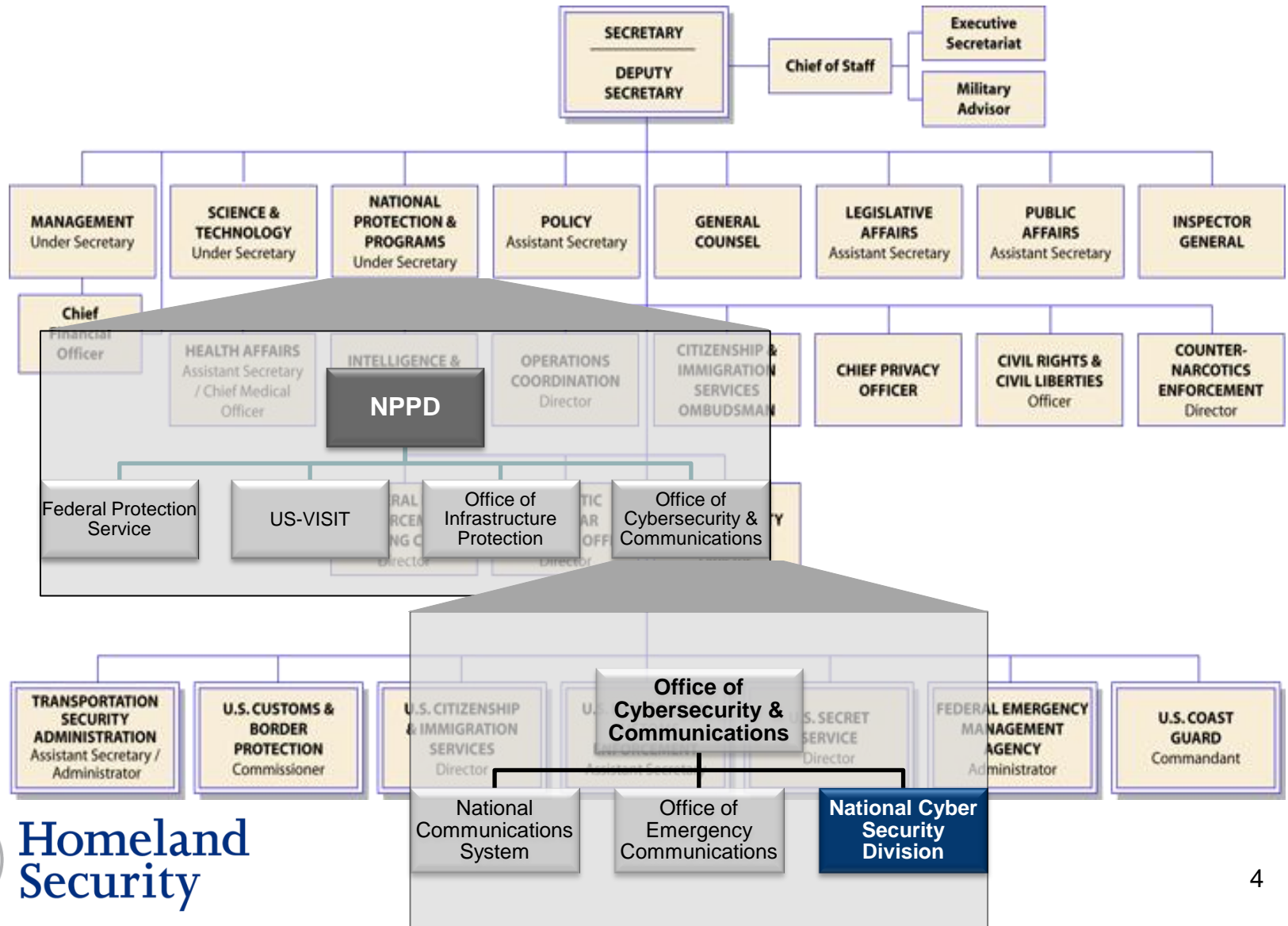
*The NIPP calls for a holistic approach to manage the risks posed to the Nation's CIKR assets, systems, networks, functions, and interconnecting links. To achieve this approach, cyber risk planners must establish, coordinate, and maintain the operations that detect and respond to cyber threats and must address large-scale capability gaps and vulnerabilities.*

## **SSAs' Primary Role**

*"Implement the NIPP framework and guidance as tailored to the specific characteristics and risk landscapes of each of the CIKR sectors."*

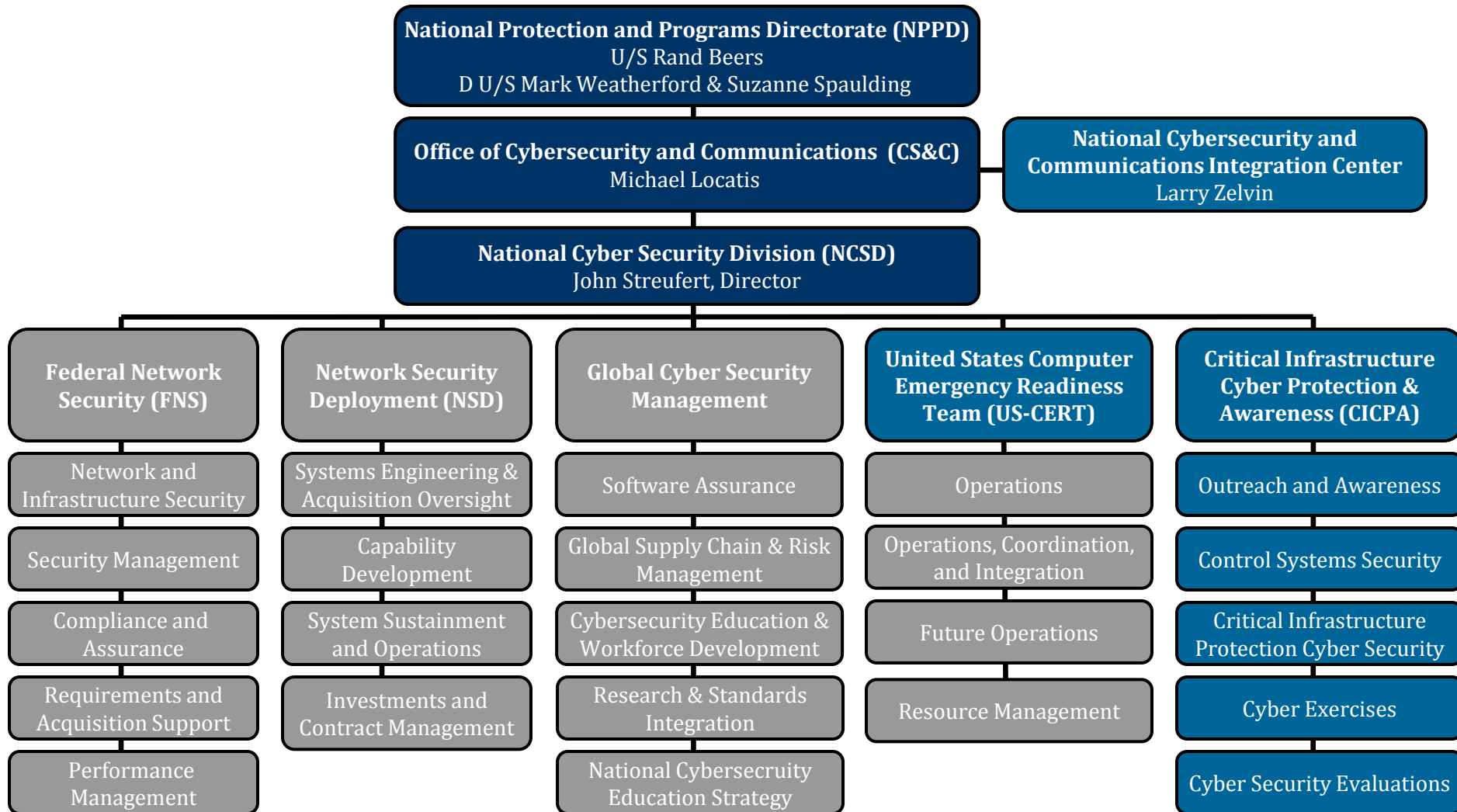


# HSPD-7 designated DHS' National Cyber Security Division (NCS) as the national focal point for securing cyberspace



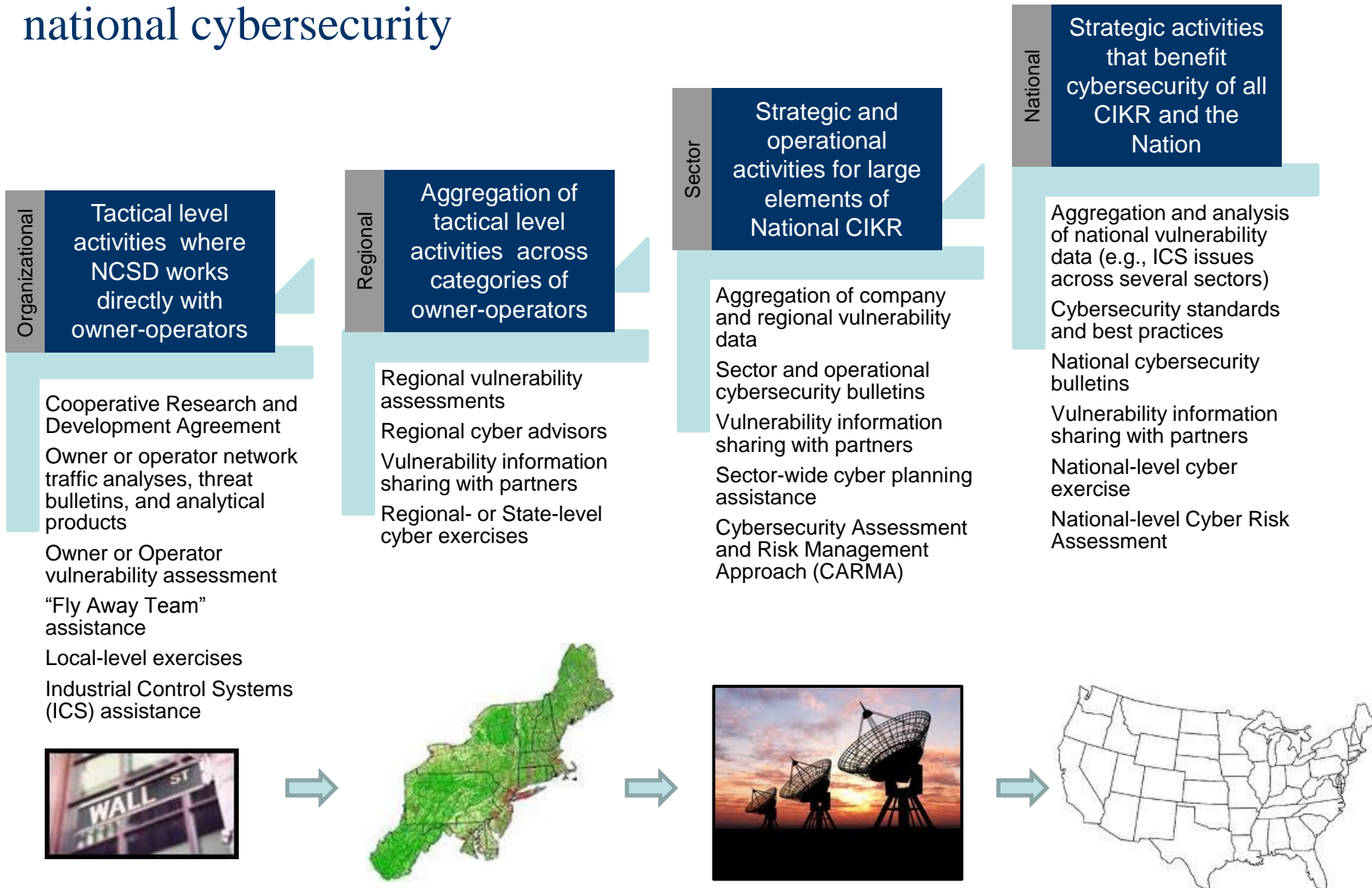
**Homeland Security**

# NCSD designates programs to work directly with private sector stakeholders to enhance organizational and national cyber resiliency

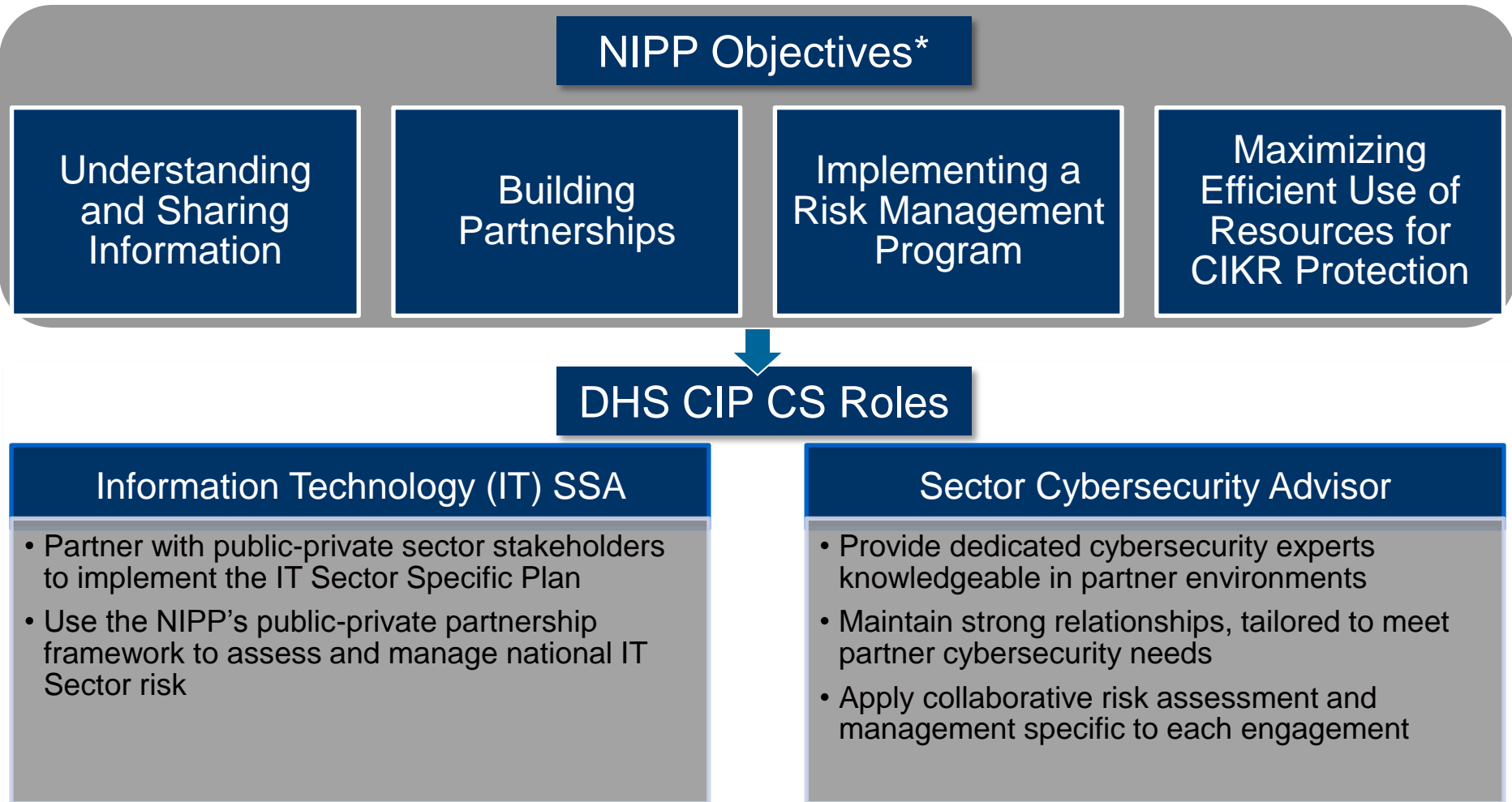


*\*While all NCSD programs interact with public and private sector partners in support of NCSD's mission, the light blue boxes represent the NCSD programs that serve as the frontline for private sector relationships*

# All of NCSD's collaborative activities drive towards greater national cybersecurity



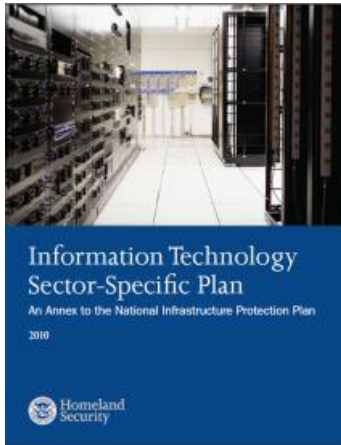
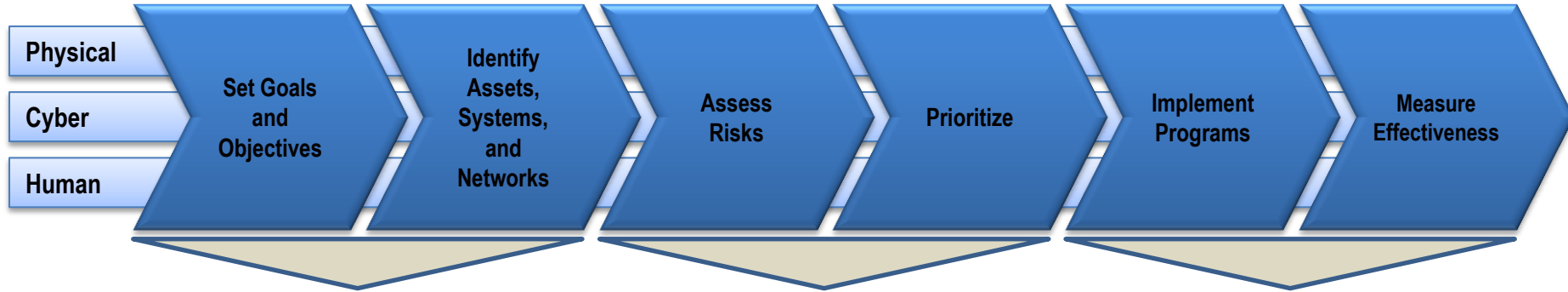
# As NCSD's lead for cybersecurity planning and strategic cyber risk management, CIP CS helps sectors meet NIPP objectives



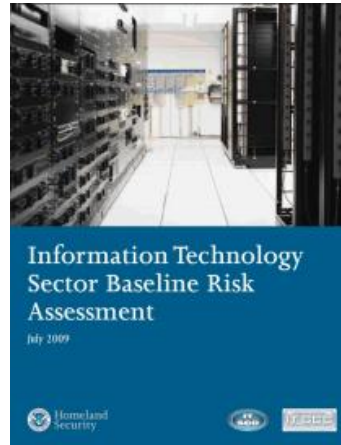


# CIP CS acts as the IT Sector Specific Agency and leads the collaborative effort to manage national IT Sector cyber risk

## Example: IT Sector Implementation of the NIPP Risk Management Framework



IT Sector mission, vision, and goals are defined in the 2007 and 2010 IT SSP



Baseline IT Sector Risk Assessment (ITSRA) completed in 2009



Information Technology Risk Management (ITSRM) strategies developed to address risks of concern identified in the ITSRA





# CIP CS applies extensive experience gained from working with IT Sector public and private partnerships to address cyber risk

IT Sector partners developed a functions-based approach for assessing and managing risk to the sector's virtual and distributed infrastructure

SMEs developed strategies to address the risks identified in the IT Sector baseline risk assessment

SMEs completed a risk assessment on the Sector's ability to provide identity management and associated trust support services

**2006**

**2007**

**2008 - 2009**

**2010 - 2011**

**2012**

Government and industry partners addressed how to implement the NIPP Risk Management Framework

More than 80 SMEs collaborated to assess risks to the IT Sector's critical functions and services:

- Produce and provide IT products and services
- Provide Domain Name Resolution Services
- Provide incident management capabilities
- Provide Internet-based content, information, and communications services
- Provide Internet routing, access, and connection services

SMEs are updating the *Provide Domain Name System (DNS) resolution services* critical function's risk profile to address changes since the 2009 baseline assessment

***The IT Sector's risk management activities have strengthened public-private partnerships and led to the development of subject matter expert (SME) communities knowledgeable in each of the sector's critical functions***



**Homeland  
Security**

# CIP CS serves as an advisor to help all sectors identify and promote cybersecurity and cyber risk management efforts

## Provide dedicated cybersecurity experts knowledgeable in partner environments

- **Benefit:** Use CIP CS cyber expertise and cross-sector experience to apply cybersecurity lessons learned, enhance information-sharing, and improve sector cyber resiliency

## Maintain strong relationships, tailored to meet partner cybersecurity needs

- **Benefit:** SSAs, public-private sector stakeholders, and SMEs can define needs and desired level of cybersecurity engagement ranging from hosting cyber webinars to conducting cyber risk management

## Apply collaborative risk assessment and management specific to each engagement

- **Benefit:** CIKR sectors are able to understand and manage cyber threats, vulnerabilities, and consequences specific to their sector at a strategic level
- **Benefit:** The risk assessment approach provides a repeatable and defensible method to efficiently plan cyber risk management activities that support sector goals and objectives



# CIP CS's Sector Engagement Strategy helps enhance the cybersecurity posture of all 18 sectors

## (I) Information-Sharing

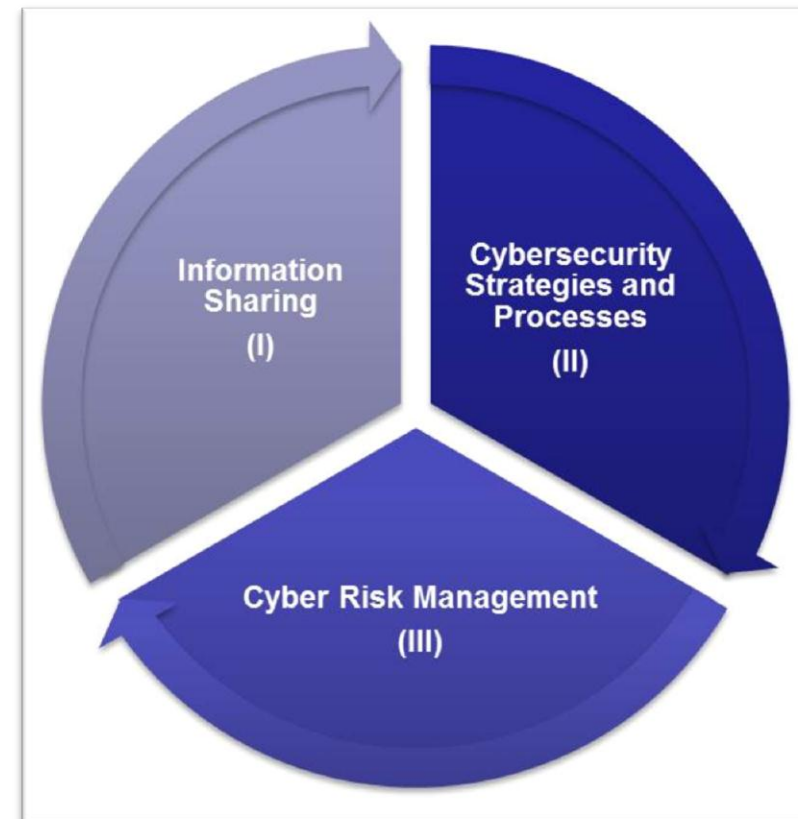
- Provide sectors with cybersecurity and NCSD information by developing cybersecurity webinars, attending GCC and SCC meetings, and sharing open-source summaries of cybersecurity news, policy, and events

## (II) Cybersecurity Strategies and Processes

- Help sectors establish cybersecurity working groups, develop and implement cybersecurity strategies, and coordinate cyber exercises

## (III) Cyber Risk Management

- Conduct a cyber risk assessment that provides a strategic view of cyber risk in a multi-risk owner environment



# In phase one, CIP CS helps sectors build a strong foundation of cybersecurity knowledge and encourage information sharing

- ▶ **Review SARs and SSPs:** Provide general feedback and suggestions on cyber topics and ideas for future cybersecurity activities
- ▶ **Attend Sector Meetings:** Participate regularly in GCC and SCC meetings to understand existing cybersecurity efforts and identify new opportunities
- ▶ **Develop Webinars:** Work with sectors to create general and issue-specific webinars on cyber topics, vulnerabilities, and mitigation efforts
- ▶ **Establish Cybersecurity Goals:** Help sectors identify and develop goals and plans to increase sector cybersecurity efforts
- ▶ **Monitor Open Source Cybersecurity Information:** Track cybersecurity news, policy, and events through open source research and develop sector-specific products to provide timely examples of relevant, specific, and reported cyber threats to the sector

## Threat: Botnets

**Botnets for Criminal Activities<sup>1</sup>**  
 In December 2010, "Operation Payback" used a 30,000-node botnet to attack PayPal and Master Card's SecureCode service. The group used a distributed denial of service (DDoS) attack, which caused the sites to go down. The group also recently attacked the Motion Picture Association of America and the websites of Senator Joseph Lieberman.

**Botnet** – a network of compromised computers able to be controlled for malicious acts, such as spamming, stealing sensitive information, DDoS, and click fraud.<sup>2</sup>

**Vulnerabilities<sup>3</sup>**

- Out-of-date anti-virus software and patches
- Opening suspicious e-mail attachments
- Clicking on links from unknown users

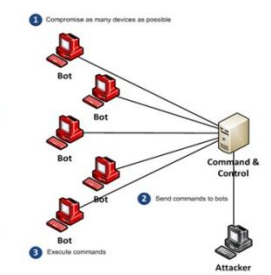


Image: SecureWorks<sup>4</sup>

---

## Threat: Botnets

**How does it work?<sup>5</sup>**

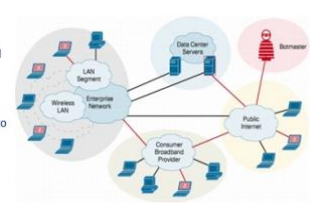
- Through a Trojan, virus, or worm, bot malware infects a computer and comes under the control of a bot master.
- The bot reports back to its master after a successful infection, staying hidden until it is ordered to carry out an attack.
- The bot master can order enslaved computers to execute malicious acts.

**What can happen to an infected computer?<sup>6</sup>**

- Infected computers can be used to send out spam, viruses, and spyware.
- Sensitive information can be stolen.
- The computer can be used as part of a DDoS attack.
- The computer can be used to carry out click fraud by automatically clicking on ads.

**Mitigation Strategies<sup>7</sup>**

- Keep anti-virus software updated and install the latest Windows patches.
- Avoid opening suspicious attachments.
- Use the highest security options in web browsers.



Source: Cisco<sup>8</sup>

**Sector(s) Affected**  
All Sectors

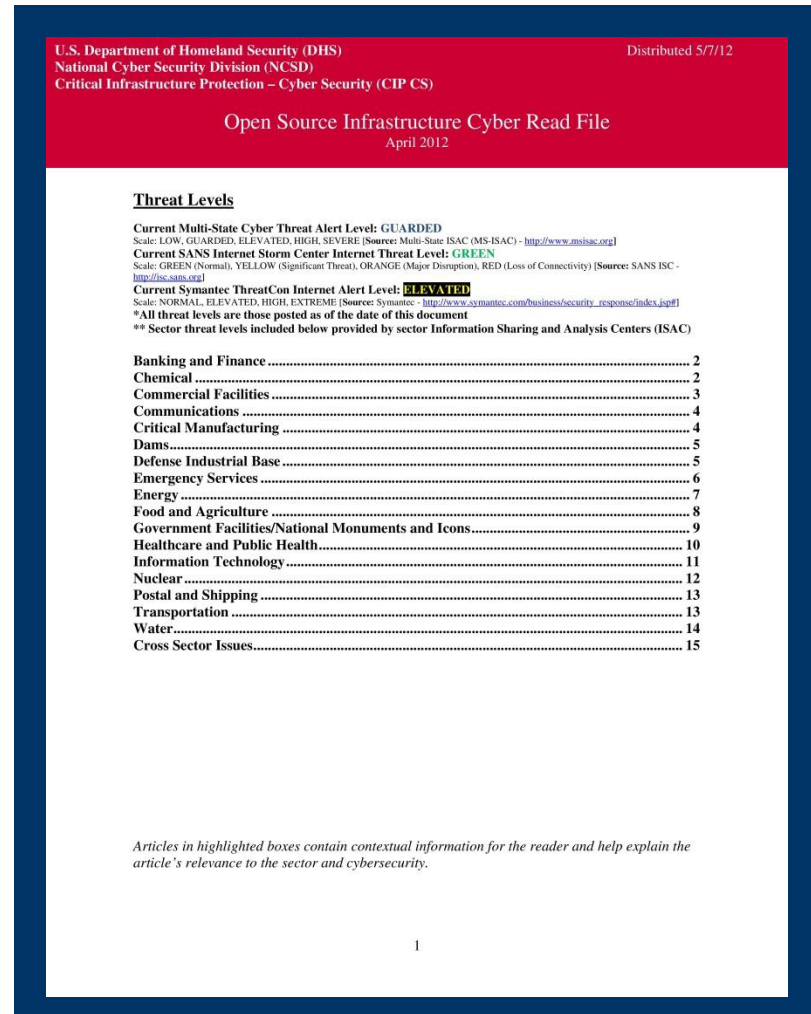
<sup>1</sup> <http://www.computer>  
<sup>2</sup> <http://us.norton.com>  
<sup>3</sup> [ibid](#)  
<sup>4</sup> <http://www.secureworks>  
<sup>5</sup> <http://us.norton.com/theme.jsp?theme=botnet>  
<sup>6</sup> [ibid](#)  
<sup>7</sup> [http://www.fsa.gov/secour/english/virus/antivirus/pdf/Bot\\_measures\\_eng.pdf](http://www.fsa.gov/secour/english/virus/antivirus/pdf/Bot_measures_eng.pdf)  
<sup>8</sup> [http://www.cisco.com/en/US/solutions/collateral/m3436/m3436r171/m3441/networking\\_solutions\\_whitepaper000ae05072a537.html](http://www.cisco.com/en/US/solutions/collateral/m3436/m3436r171/m3441/networking_solutions_whitepaper000ae05072a537.html)

**Homeland Security**

Example of a threat presentation on botnets

# CIP CS Open Source Infrastructure Cyber Read File provides timely examples of relevant, specific, and reported threats

- ▶ Increase understanding of current issues and threat trends
- ▶ Convey the reality of cyber threats and the importance of addressing cybersecurity through current events
- ▶ Provide overarching sector cybersecurity trends to guide other cyber efforts
- ▶ Use to inform cyber exercise planning and other sector cybersecurity initiatives





# The Read File content is organized by sector and includes added contextual information that can help inform strategic planning

- The Read File focuses on cybersecurity and cyber infrastructure
- The layout is modeled after DHS's Daily Open Source Infrastructure Report

- Articles come from open source news resources and are organized by date and the sector(s) they affect

## Banking and Finance

### Current Financial Services Cyber Threat Alert Level: GUARDED

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Financial Services (FS-ISAC) - <http://www.fsisac.com>]

**April 17, CSO – (National) Paying with smartphones to outpace credit cards by 2020, experts say.** Source: <http://www.csoonline.com/article/704419/paying-with-smartphones-to-outpace-credit-cards-by-2020-experts-say>

**Scope:** International

**Context:** A survey found that payments using near field communications (NFC) in smartphones and payment terminals would become more popular than cash and credit card payments by 2020. While NFC payments are increasing in popularity, security concerns about protecting the data passed from a phone to a payment terminal remain. With concerns that smartphones are vulnerable to eavesdropping and that data transmissions are vulnerable to interception, NFC payments are likely to become popular targets for malicious actors, especially if NFC payments become widespread.

**April 12, The Register – (International) Banks on the business end of DDoS attack surge – report.** Source: [http://www.theregister.co.uk/2012/04/12/prolexic\\_ddos\\_trends/](http://www.theregister.co.uk/2012/04/12/prolexic_ddos_trends/)

**Scope:** International

**Context:** According to a report written by a firm specializing in distributed denial of service (DDoS) mitigation, banks are increasingly the targets of DDoS attacks, with a dramatic increase in the number of malicious packet traffic aimed at banks over the past year. The findings of this report highlight the efficacy of DDoS attacks. On one hand, a simple DDoS attack can block customer access to a banking website. On the other, DDoS attacks can be used as a distraction to hide other, more serious attacks that steal proprietary or customer information. Because DDoS attacks can be used to achieve a variety of end goals, this upward trend is likely to continue.

**April 12, The Register – (Japan) Japanese bank palms off customers with biometric ATMs.** Source: [http://www.theregister.co.uk/2012/04/12/ogaki\\_palm\\_scanning\\_cash/](http://www.theregister.co.uk/2012/04/12/ogaki_palm_scanning_cash/)

**Scope:** International

**Context:** A Japanese bank has introduced biometric authentication technology for ATM services. Rather than using an ATM card, customers can use just their handprints to withdraw cash or perform other banking functions. The gradual introduction of biometrics for authentication purposes may lead to more secure transactions in the Banking and Finance Sector, though the collection, storage, and use of biometric data by private sector organizations will be an important cybersecurity issue.

**April 11, Dark Reading – (International) Zeus Trojan targets online payroll services providers.** Source: <http://www.darkreading.com/advanced-threats/167901091/security/attacks-breaches/232900036/zeus-trojan-targets-online-payroll-services-providers.html>

**Scope:** National

**Context:** Zeus-based attacks are evolving from stealing banking information to stealing login information for cloud-based payroll services. By targeting payroll services, hackers can add money mules, or people paid by criminals to launder illicit funds, as employees and funnel stolen funds quickly to their bank accounts. Because businesses often have larger sums of money than individual bank account holders, cloud-based payroll companies serving those businesses may become increasingly attractive targets.

**April 23, CSO – (International) European Central Bank calls for feedback on internet payments security advice.** Source: <http://www.csoonline.com/article/704766/european-central-bank-calls-for-feedback-on-internet-payments-security-advice>

**April 19, Bank Info Security – (National) ATM attacks exploit lax security.** Source: <http://www.bankinfosecurity.com/atm-attacks-exploit-lax-security-a-4689>

**April 16, ZDNet – (International) 3 million bank accounts hacked in Iran.** Source: <http://www.zdnet.com/blog/security/3-million-bank-accounts-hacked-in-iran/11577>

- Added context helps increase understanding of how cybersecurity impacts critical infrastructure protection efforts
- Context is developed by CIP CS cybersecurity experts knowledgeable in sector environments

*The Read File is posted to the CIP CS Homeland Security Information Network Critical Sectors (HSIN-CS) page on a monthly basis and may be distributed by sectors and federal and state governments to their stakeholders.*

<https://cs.hsin.gov/sites/CIP-CS/default.aspx>

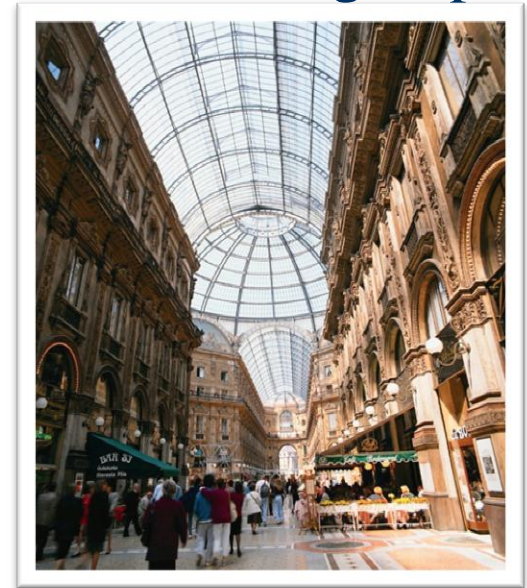


**Homeland Security**

# CASE STUDY: Cyber-focused activities helped the Commercial Facilities Sector connect with a large, diverse stakeholder group

## Process

- ▶ Developed tailored cybersecurity webinars to engage the Retail and Gaming Subsectors
- ▶ Distributed open-source reports that identified recent sector cybersecurity threats
- ▶ Established a Commercial Facilities Working Group to facilitate ongoing cybersecurity collaboration



## Outcomes

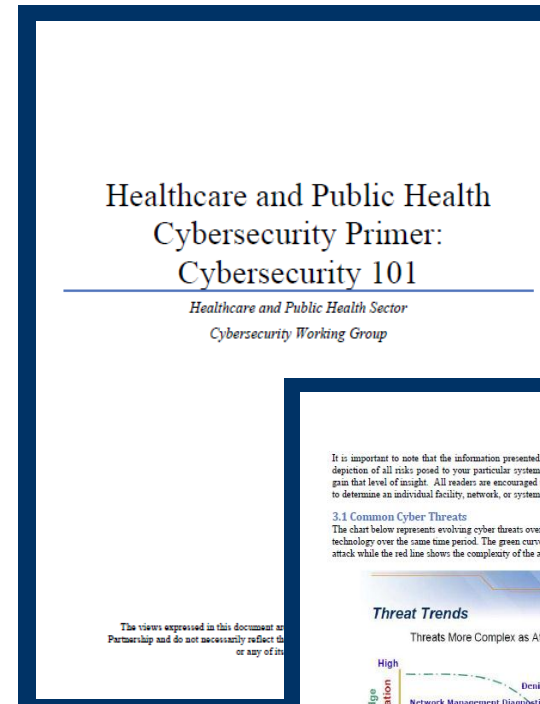
- ▶ Engaged more than 100 participants in a cybersecurity Webinar discussion
- ▶ Generated interest and helped identified potential sector stakeholders to participate in the cyber working group from the Webinar attendee list
- ▶ Increased awareness of potential cyber vulnerabilities and cybersecurity threats in the Retail, Gaming, and Entertainment and Media Subsectors
- ▶ Established a process to engage Commercial Facilities stakeholders on a regular basis with the newly formed Commercial Facilities Cyber Working Group



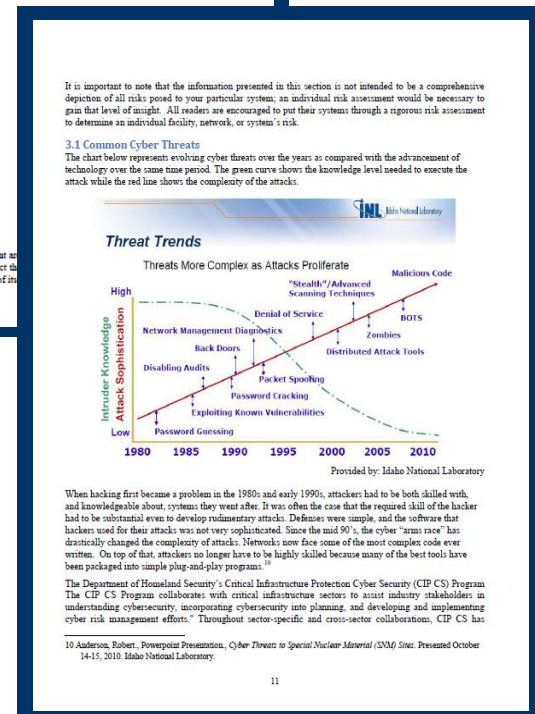


# In phase two, CIP CS helps sectors develop cybersecurity strategies and overarching processes

- ▶ **Define Cybersecurity Goals:** Help sectors identify and develop goals and plans to increase sector cybersecurity efforts
- ▶ **Establish Cyber Working Groups:** Provide training materials, agenda suggestions, and speakers to assist sectors in establishing and maintaining their cyber working groups
- ▶ **Develop a Cybersecurity Strategy:** Help sectors develop and pursue strategies to explain sector goals and outline plans to meet them
- ▶ **Provide Assessment Tool Input:** Provide cybersecurity input to help ensure sector risk self-assessment tools address all hazards
- ▶ **Help Plan Cyber Exercises:** Coordinate with the NCSD Cyber Exercise Program to assist sectors with planning and implementing cyber exercises



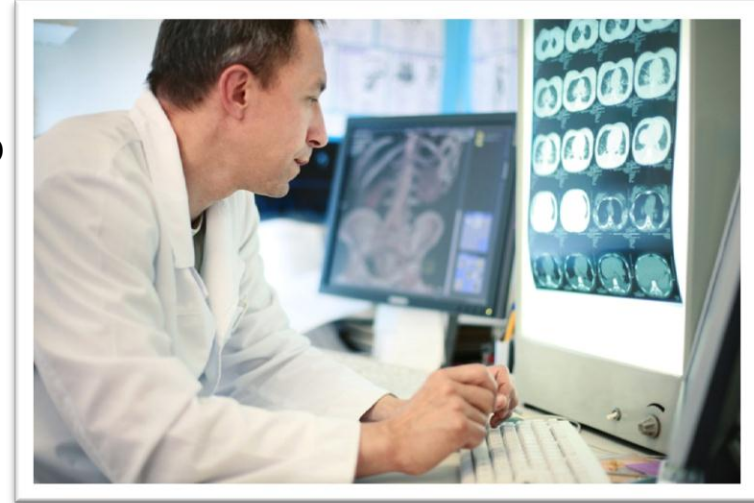
The views expressed in this document as Partnership and do not necessarily reflect the or any of its



# CASE STUDY: The Healthcare and Public Health Sector Primer established a baseline cybersecurity overview for the sector

## Process

- ▶ Provided input to goals, objectives, and year-long plan for the sector's Cyber Security Working Group
- ▶ Distributed open-source reports that identified recent sector cybersecurity threats
- ▶ Provided national-level cybersecurity context for Primer sections such as information sharing, cyber risk management, and cybersecurity education



## Outcomes

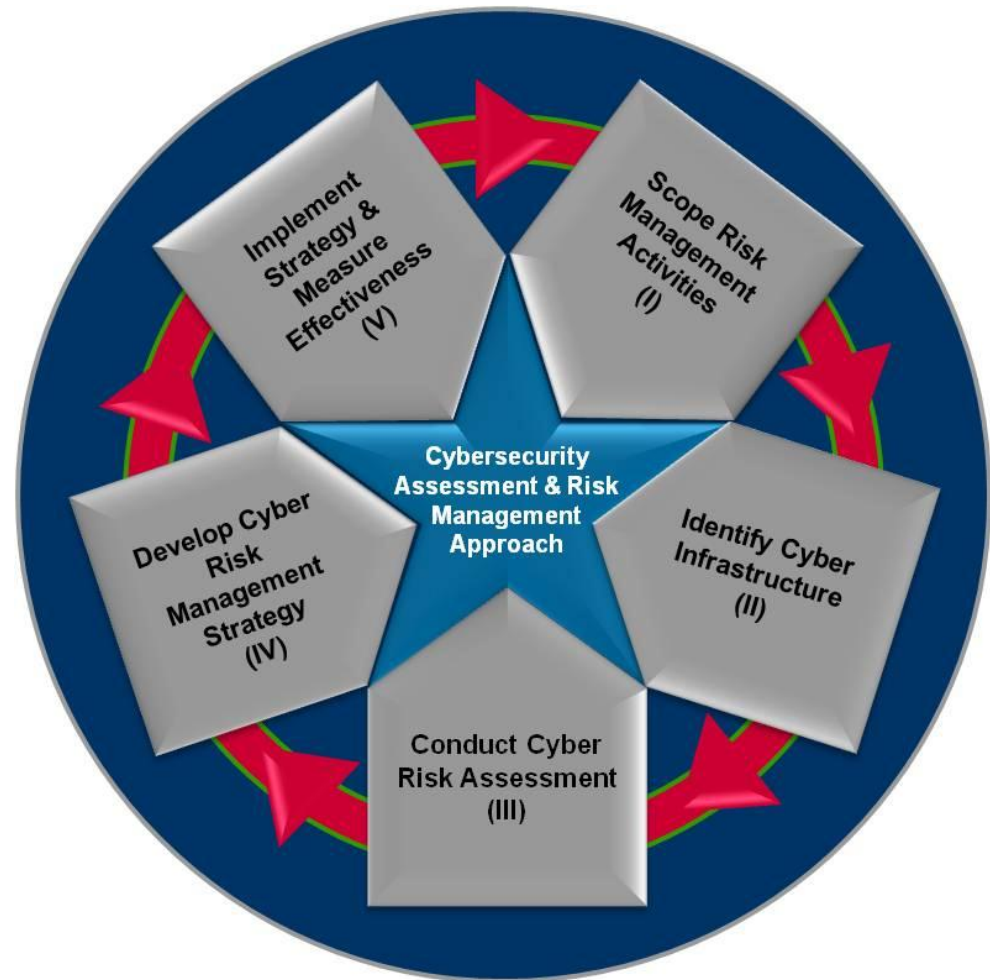
- ▶ Engaged with participants from various subsectors in a cybersecurity discussion
- ▶ Connected the Sector Specific Agency with resources and additional materials to build Primer content
- ▶ Increased awareness of potential cyber vulnerabilities and cybersecurity threats
- ▶ The sector produced an educational document on cybersecurity for Healthcare and Public Health Sector members across the nation



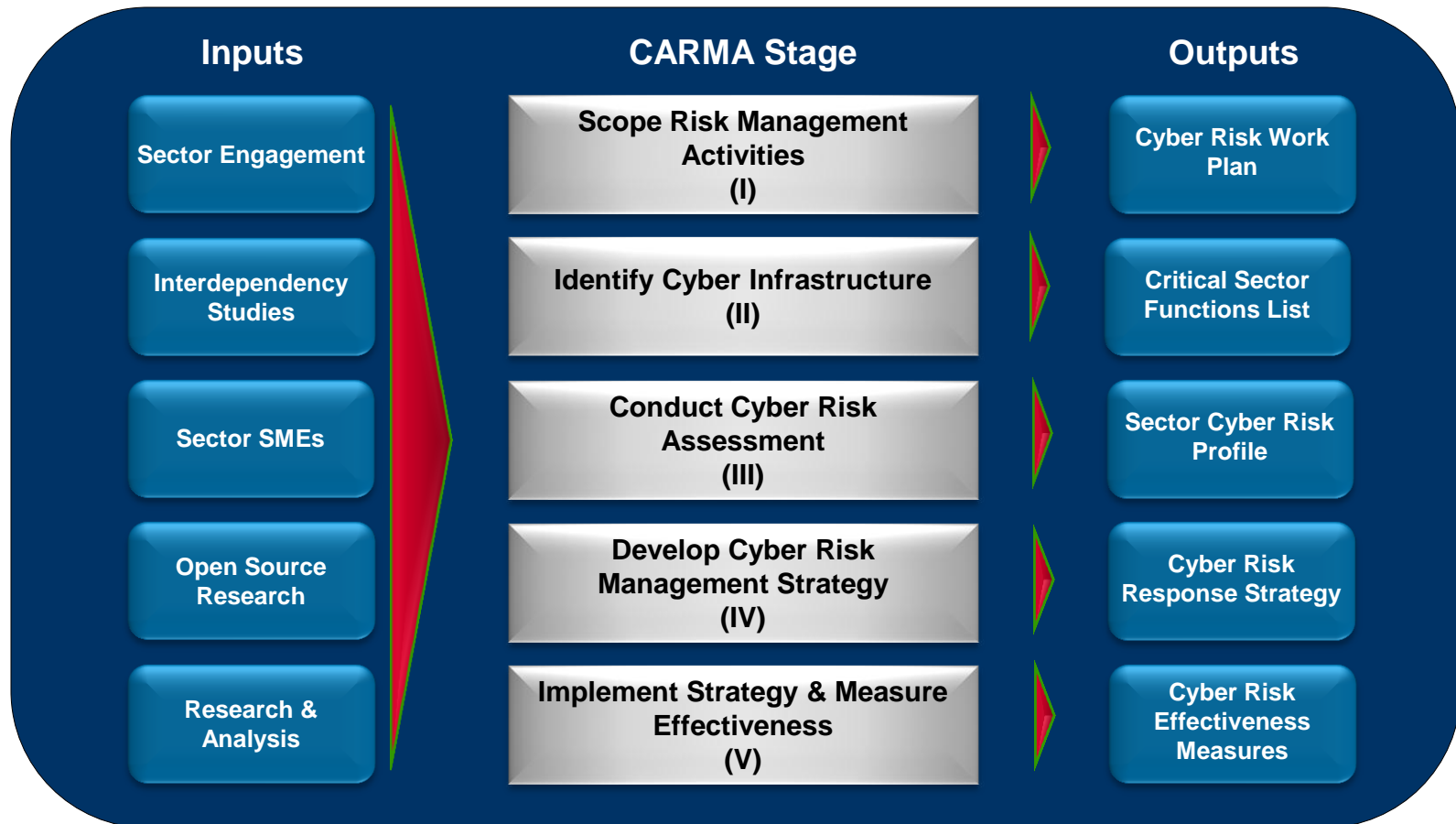
In phase three, CARMA provides sectors with a strategic view of cyber risk that addresses the complexity of cyberspace

### Cybersecurity Assessment and Risk Management Approach (CARMA)

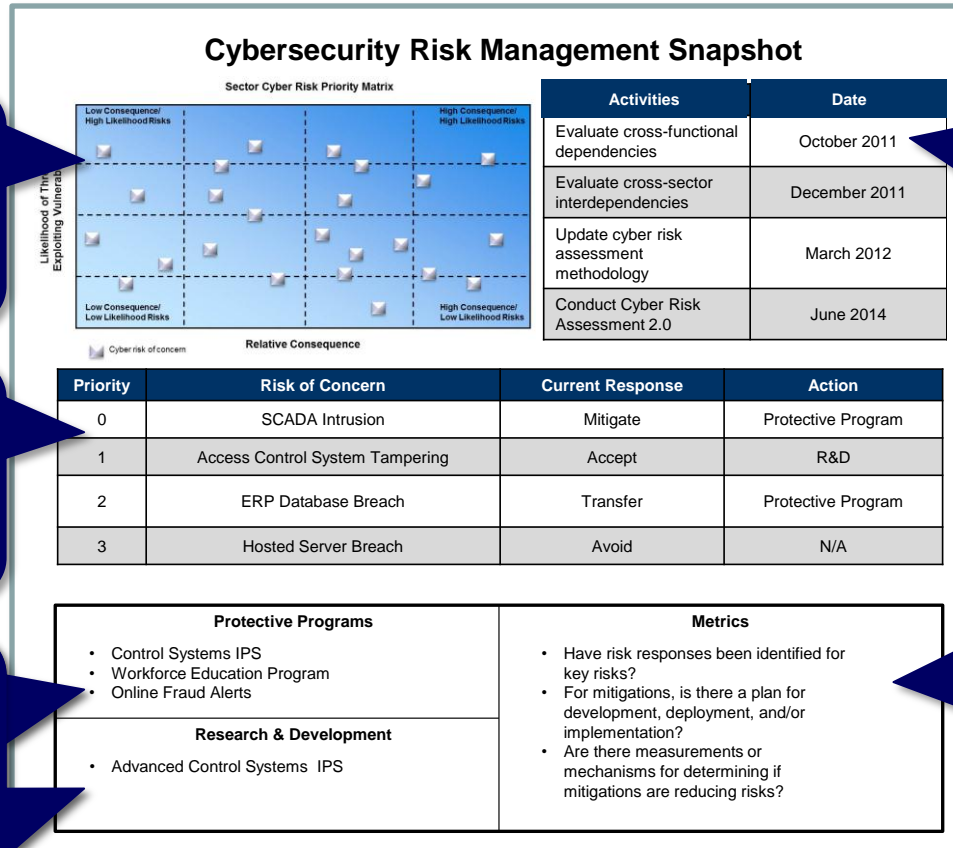
- Enables partners to effectively identify, assess, and manage national level cyber risks to their infrastructure
- Assists partners in assessing cyber threats, vulnerabilities, and consequences to formulate a cyber risk profile
- Allows partners to identify best practices, programs, subject matter experts, and partners to manage cyber risks to mitigate cyber risk impact to their mission



# CARMA relies on a variety of sources to produce cyber risk management materials that address a sector's critical functions



# CARMA results provide CIKR partners tangible cyber risk analyses and management strategies



**Risk Priority Matrix**

- Summarizes risks to the most basic level
- Prioritizes risks by showing relative likelihood and consequence evaluations

**Risk Response Table**

- Summarizes strategy for managing identified risks
- Risk response options can be: accept; avoid; transfer; or mitigate.

**List of Relevant Protective Programs and R&D**

- Captures key initiatives that seek to address risks
- Captures research and development (R&D) efforts that seek to address risks

**Future Risk Activities Table**

- Summarizes areas for future evaluation
- Provides a snapshot of key milestones for risk management activities

**Cybersecurity Metrics List/Dashboard**

- Articulates the measurements that evaluate risk response implementation
- Can be displayed in list or dashboard format

**NOTE:** To view an example of what an end product of the assessment can look like, please visit the following link to the IT Sector Baseline Risk Assessment (August 2009): [http://www.dhs.gov/xlibrary/assets/nipp\\_it\\_baseline\\_risk\\_assessment.pdf](http://www.dhs.gov/xlibrary/assets/nipp_it_baseline_risk_assessment.pdf). To view an example of what a risk management strategy can look like, please visit the following link to the Domain Name System Risk Management Strategy (June 2011): <http://www.dhs.gov/xlibrary/assets/it-sector-risk-management-strategy-domain-name-resolution-services-june2011.pdf>

This is not a prescriptive format to follow; just an example. All CARMA evaluations will likely be different and result in unique end products that meet the needs of the stakeholder group conducting the assessment.





# CASE STUDY: Emergency Services Sector (ESS) jurisdictions used CARMA to strategically and uniformly address cyber risk

## Process

- ▶ Recruited members from the six ESS disciplines to work to identify, prioritize, and manage cyber risks
- ▶ CARMA solicited input on widely impactful nationwide threats, vulnerabilities, and consequences through seven targeted evaluation sessions and scenarios
- ▶ CARMA's flexibility addressed the ESS' public-service mission to protect citizens and other sectors

*"The CARMA methodology has helped ESS work collectively as a large, dispersed group of public partners from across the country. By focusing on cyber risk in manageable phases, we are better able to understand and address our sector's complex, cyber dependencies and interdependencies."*

*- Mark Hogan, Co-Chair, ESS Cyber Security Working Group*

## Outcomes

- ▶ Conducting CARMA fostered greater cyber collaboration between ESS stakeholders from diverse districts and disciplines
- ▶ The finalized list of critical ESS functions and associated cyber infrastructure informs a sector-wide, cyber risk profile which will help determine appropriate incident response
- ▶ CARMA will help the sector prioritize risks of concern and determine where to focus their cyber efforts and will link to the ESS cybersecurity roadmap\*



## Conclusion

- ▶ Cybersecurity planning and cyber risk management efforts address NIPP requirements and are an important part of critical infrastructure protection
- ▶ CIP CS applies experience and lessons learned from working with the sectors since DHS's inception to enhance sector cyber resiliency
- ▶ CIP CS cyber experts are available to collaborate on cybersecurity planning efforts and cyber risk assessments that meet individual sector needs

For more information, please contact:

**Thad Odderstol**

CIP CS Program Director

[Thad.Odderstol@dhs.gov](mailto:Thad.Odderstol@dhs.gov)

**Jason Gates**

CIP CS Program Analyst

[Jason.Gates@dhs.gov](mailto:Jason.Gates@dhs.gov)

*The CIP CS Program is part of the National Cyber Security Division's Office of Cybersecurity and Communications within the Department of Homeland Security's National Protection and Programs Directorate.*



**Homeland  
Security**





Homeland  
Security