Cyber Risk Management

Presenter: LCDR Josh Rose & LT Josie Long

Critical Infrastructure Protection Branch Chief

Office of Port & Facility Compliance (CG-FAC)

AAPA Cybersecurity Seminar 11-12 March 2015

The Evolving Threat…Call to Action

"Cybersecurity is one of the most serious economic and national security challenges we face as a nation…"

- President Obama, February 2013

"We are all connected online and a vulnerability in one place can cause a problem in many other places. So everyone needs to work on this: government officials and business leaders, security professionals and utility owners and operators." *- DHS Secretary Jeh Johnson, February 2014*

"The loss of industrial information and intellectual property through cyber espionage constitutes the greatest transfer of wealth in history."

- General Alexander, August 2013

"Cyber affects the full spectrum of Coast Guard operations…it cuts across every aspect of the Coast Guard. We all have a role in cybersecurity and protection of our networks, and we must treat them like the mission-critical assets that they are."

- Admiral Zukunft, September 2014

Policies, Directives and Mandates

Presidential / National Policy

NATIONAL SECURITY STRATEGY

May 2010

THE NATIONAL STRATEGY TO SECURE CYBERSPACE

FEBRUARY 2003

THE WHITE HOUSE

Office of the Press Secretary

EMBARGOED UNTIL DELIVERY OF THE PRESIDENT'S STATE OF THE UNION ADDRESS February 12, 2013

February 12, 2013

PRESIDENTIAL POLICY DIRECTIVE/PPD-21

SUBJECT: Critical Infrastructure Security and Resilience

The Presidential Policy Directive (PPD) on Critical Infrastructure Security and Resilience advances a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure.

Introduction

The Nation's critical infrastructure provides the essential services that underpin American society. Proactive and coordinated efforts are necessary to strengthen and maintain secure, functioning, and resilient critical infrastructure – including assets, networks, and systems – that are vital to public confidence and the Nation's safety, prosperity, and well-being.

[illegible]

Presidential Documents

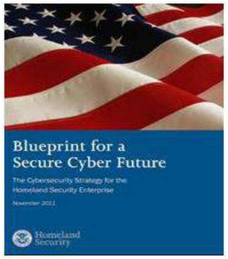
Title 3— The President

Executive Order of February 12, 2013

Improving Critical Infrastructure Cybersecurity

[illegible]

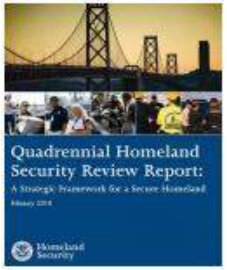
DHS Policies / Directives


Blueprint for a Secure Cyber Future

The Cybersecurity Strategy for the Homeland Security Enterprise

November 2011

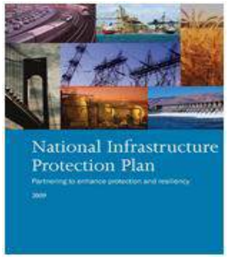
Homeland Security


Quadrennial Homeland Security Review Report:

A Strategic Framework for a Secure Homeland

February 2010

Homeland Security


National Infrastructure Protection Plan

Partnering to enhance protection and resiliency

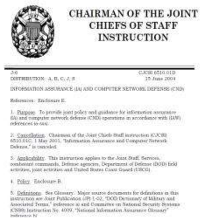
2009

DOD Policies / Directives

Joint Publication 3-13

Information Operations

27 November 2012


CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J-6 CJCSI 6510.01D
DISTRIBUTION: A, B, C, J, S 15 June 2004

INFORMATION ASSURANCE (IA) AND COMPUTER NETWORK DEFENSE (CND)

References: Enclosure E.

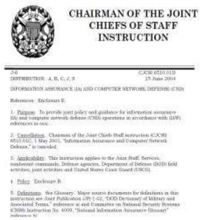
1. Purpose. To provide joint policy and guidance for information assurance (IA) and computer network defense (CND) operations in accordance with (IAW) references a-aaa.

2. Cancellation. Chairman of the Joint Chiefs Staff instruction (CJCSI) 6510.01C, 1 May 2001, "Information Assurance and Computer Network Defense," is canceled.

3. Applicability. This instruction applies to the Joint Staff, Services, combatant commands, Defense agencies, Department of Defense (DOD) field activities, joint activities and United States Coast Guard (USCG).

4. Policy. Enclosure B.

5. Definitions. See Glossary. Major source documents for definitions in this instruction are Joint Publication (JP) 1-02, "DOD Dictionary of Military and Associated Terms," (reference a) and Committee on National Security Systems (CNSS) Instruction No. 4009, "National Information Assurance Glossary" (reference b).


CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J-6 CJCSI 6510.01D
DISTRIBUTION: A, B, C, J, S 15 June 2004

INFORMATION ASSURANCE (IA) AND COMPUTER NETWORK DEFENSE (CND)

References: Enclosure E.

1. Purpose. To provide joint policy and guidance for information assurance (IA) and computer network defense (CND) operations in accordance with (IAW) references a-aaa.

2. Cancellation. Chairman of the Joint Chiefs Staff instruction (CJCSI) 6510.01C, 1 May 2001, "Information Assurance and Computer Network Defense," is canceled.

3. Applicability. This instruction applies to the Joint Staff, Services, combatant commands, Defense agencies, Department of Defense (DOD) field activities, joint activities and United States Coast Guard (USCG).

4. Policy. Enclosure B.

5. Definitions. See Glossary. Major source documents for definitions in this instruction are Joint Publication (JP) 1-02, "DOD Dictionary of Military and Associated Terms," (reference a) and Committee on National Security Systems (CNSS) Instruction No. 4009, "National Information Assurance Glossary" (reference b).

CG Policies / Directives

BEING DEVELOPED

USCG CYBER STRATEGY

25 April 2014 – Version 3

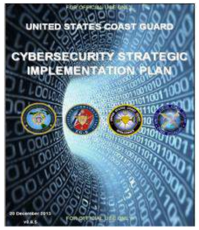
United States Coast Guard

Cyber Strategy

DRAFT

April 2014
Washington, D.C.

DISCUSSION DRAFT – PRE-DECISIONAL – EMBARGOED FROM PUBLIC RELEASE


FOR OFFICIAL USE ONLY

UNITED STATES COAST GUARD

CYBERSECURITY STRATEGIC IMPLEMENTATION PLAN

20 December 2013

v0.8.5

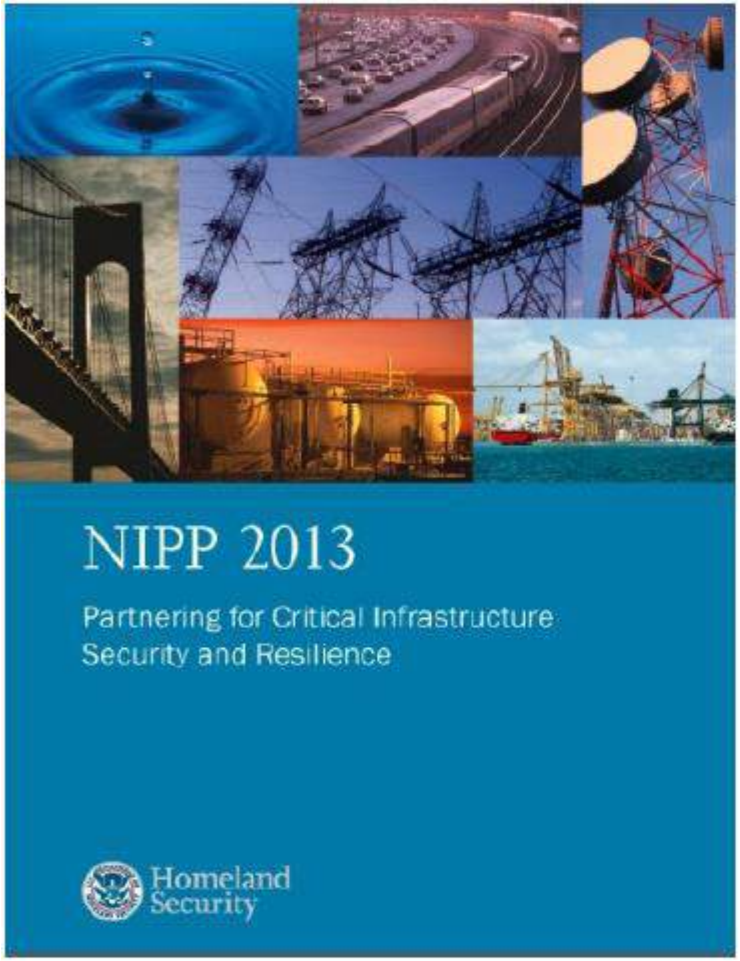
FOR OFFICIAL USE ONLY

NVIC

Maritime Critical Infrastructure

The Coast Guard is the Sector Specific Agency (SSA) for the Maritime component of the Transportation Sector

- 1 of the 16 Critical Sectors
- Collaboration with our partners in TSA and DOT
- Protect maritime sector from all threats (physical, personnel, and ***cyber***)



NIPP 2013

Partnering for Critical Infrastructure Security and Resilience

Homeland Security

EO 13636

- **EO 13636: Improving Critical Infrastructure Cybersecurity Directs the Executive Branch to:**
  - Develop a technology-neutral voluntary cybersecurity framework
  - Promote and incentivize the adoption of cybersecurity practices
  - Increase the volume, timeliness and quality of cyber threat information sharing
  - Incorporate strong privacy and civil liberties protections into every initiative to secure our critical infrastructure
  - Explore the use of existing regulation to promote cyber security

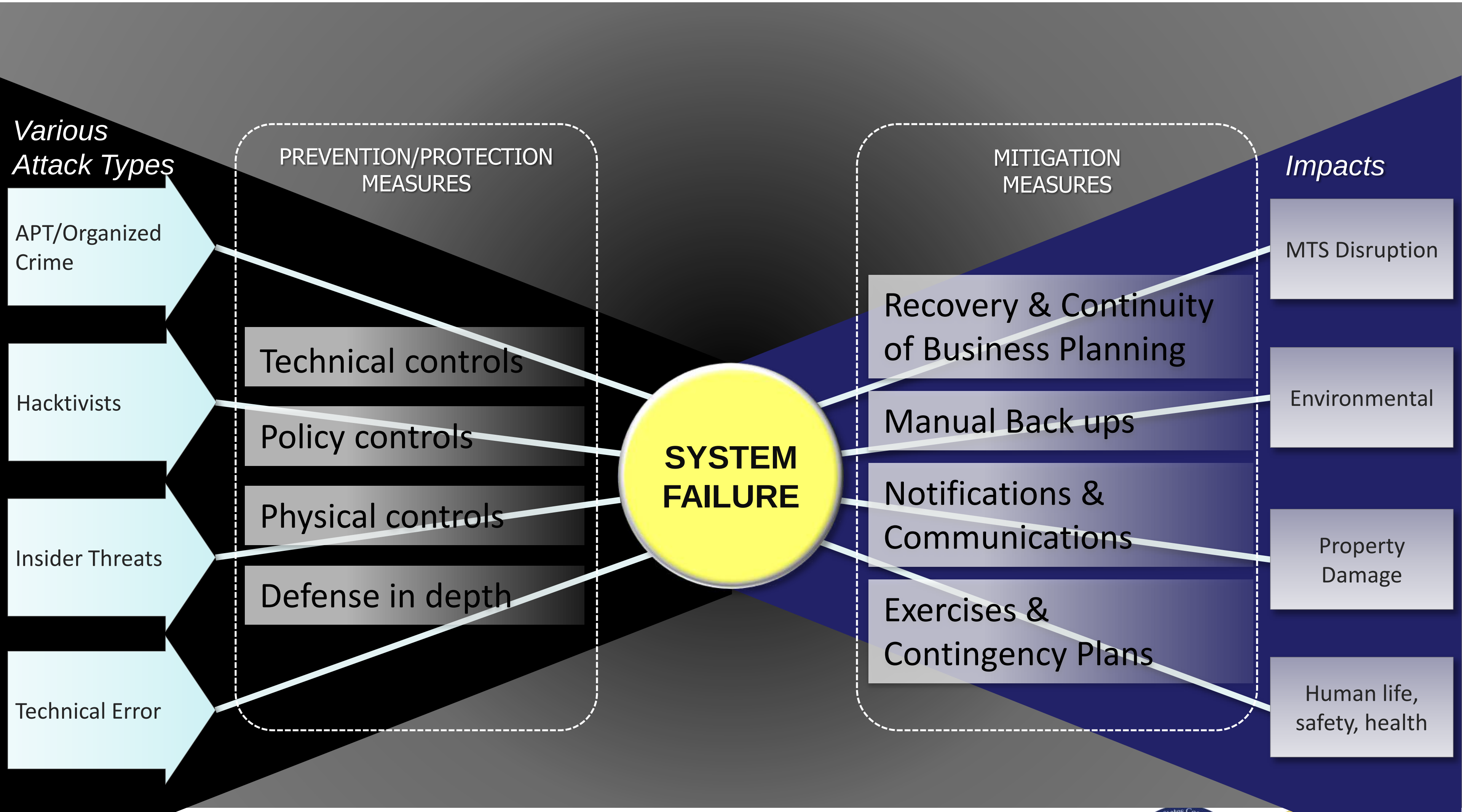
PPD-21

- **Presidential Policy Directive-21: Critical Infrastructure Security and Resilience replaces Homeland Security Presidential Directive-7 and directs the Executive Branch to:**
- Develop a situational awareness capability that addresses both physical and cyber aspects of how infrastructure is functioning in near-real time
- Understand the cascading consequences of infrastructure failures
- Evaluate and mature the public-private partnership
- Update the National Infrastructure Protection Plan
- Develop comprehensive research and development plan

Coast Guard Cyber Strategy

- 3 Priorities:
  1. Defending Cyberspace in USCG
  2. Enabling Operations
  3. Protecting Infrastructure
     1. Promote Cyber Risk Awareness & Management
     2. Prevent: Reduce Cyber Vulnerabilities in the MTS

Cyber Security Risk Model



Various Attack Types

- APT/Organized Crime
- Hacktivists
- Insider Threats
- Technical Error

PREVENTION/PROTECTION MEASURES

- Technical controls
- Policy controls
- Physical controls
- Defense in depth

SYSTEM FAILURE

MITIGATION MEASURES

- Recovery & Continuity of Business Planning
- Manual Back ups
- Notifications & Communications
- Exercises & Contingency Plans

Impacts

- MTS Disruption
- Environmental
- Property Damage
- Human life, safety, health

All activities must take place against a backdrop of the training, education, and policies needed to promote a culture of cyber security

Threat Actors

Criminals

Insiders

Nation-states

Self-inflicted

Natural

Hacktivists

Ongoing Initiatives

- The USCG Cyber Strategy
- Continue to evaluate and distribute voluntary risk assessment tools to industry
- Draft guidance for industry on risk reduction
- Clarify notification procedures

NVIC: VOLUNTARY GUIDANCE

- How do we incorporate cyber into risk assessments?
- What tools are available for industry to use for risk assessments?
- MTS standard terms (definitions)
- What are examples of industrial control systems in the maritime environment (what is the scope of NVIC)?

NIST FRAMEWORK

Identify	What assets need protection?
Protect	What safeguards are available?
Detect	What techniques can identify incidents?
Respond	What techniques can contain impacts of incidents?
Recover	What techniques can restore capabilities?

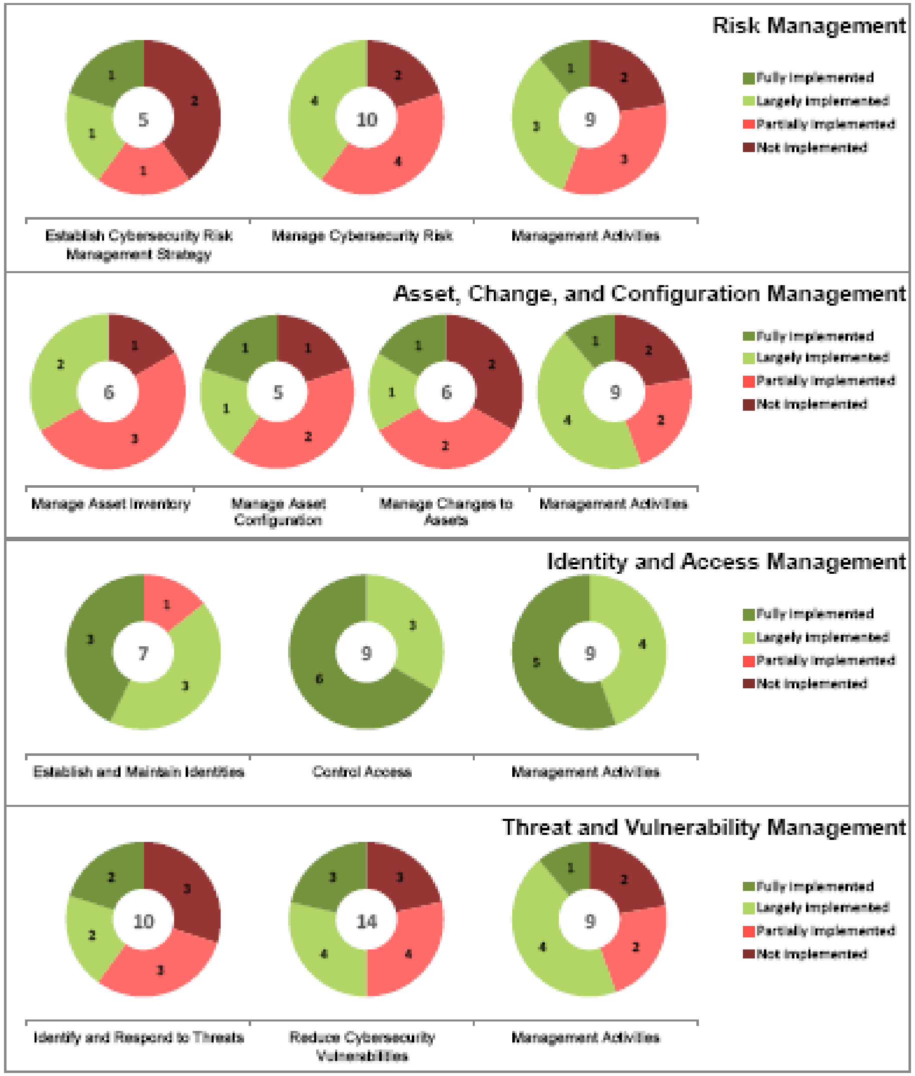
Framework can be found at:
http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

Cyber Capability Maturity Model

Department of Energy Tool originally developed pre-NIST

Worked with DHS and DOE to develop a maritime version

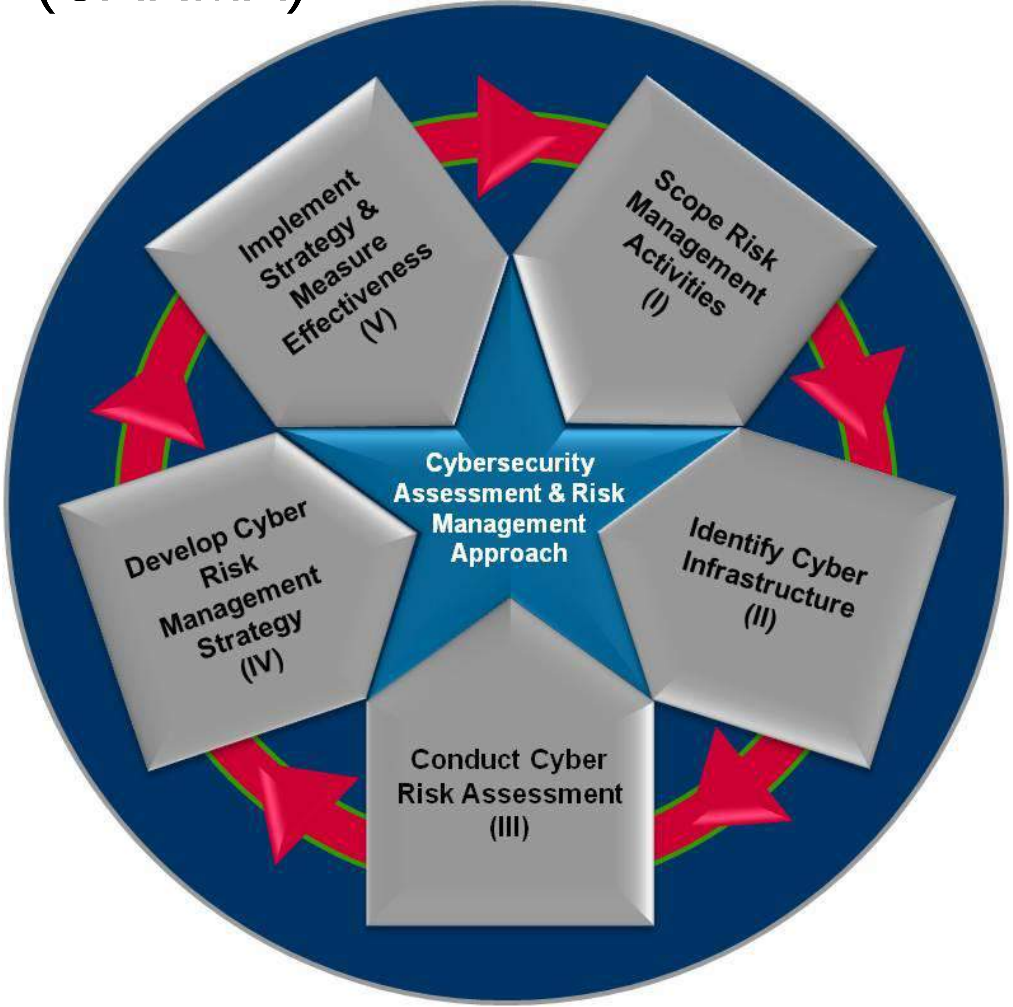
Beta test successfully completed with a maritime company



Cyber Security Assessment and Risk Management Approach

(CARMA)

- System used to evaluate national level cyber CI risks to meet Executive Order requirements
- Worked with DHS to develop a port-level version
- Beta testing will be conducted at a port later this year.


Cybersecurity Assessment & Risk Management Approach
Scope Risk Management Activities (I)
Identify Cyber Infrastructure (II)
Conduct Cyber Risk Assessment (III)
Develop Cyber Risk Management Strategy (IV)
Implement Strategy & Measure Effectiveness (V)

PUBLIC MEETING ON 15 JAN

The Coast Guard is seeking public input on the following questions:

(1) What cyber-dependent systems, could lead to a TSI?

(2) What procedures or standards are used to id cybersecurity vulnerabilities?

(3) Are there existing cybersecurity assurance programs available?

(4) Cyber security training programs?

(5) When are manual backups or other non-technical approaches needed?

(6) How can Alternative Security Programs be used?

(7) How can Coast Guard verify technical or procedural standards?

(8) How do third parties (class, insurance, etc) play a role?

https://www.federalregister.gov/articles/2014/12/12/2014-29205/guidance-o n-maritime-cybersecurity-standards

Incident Response: Resources

- National Response Center ((800) 424-8802)

– Local COTP

- National CyberSecurity and Communications Integration Center (NCCIC)
  - 16 sectors, law enforcement, CERTS
  - Unified Coordination Group
  - NCCIC@hq.dhs.gov

- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
  - Incident response specific to SCADA and Control Systems
  - ICS-CERT@hq.dhs.gov

- United States Computer Emergency Readiness Team (US-CERT)
  - Incident response across the Enterprise
  - www.us-cert.gov

FY2014 PSGP Cyber Projects Summary

- ❑ Port Security Grant Program
  - Established by MTSA 2002
  - COTP/AMSC/PSS reviewed, scored, and prioritized grantee projects,
  - CGHQ & both CG Areas sit on the National Review Panel.

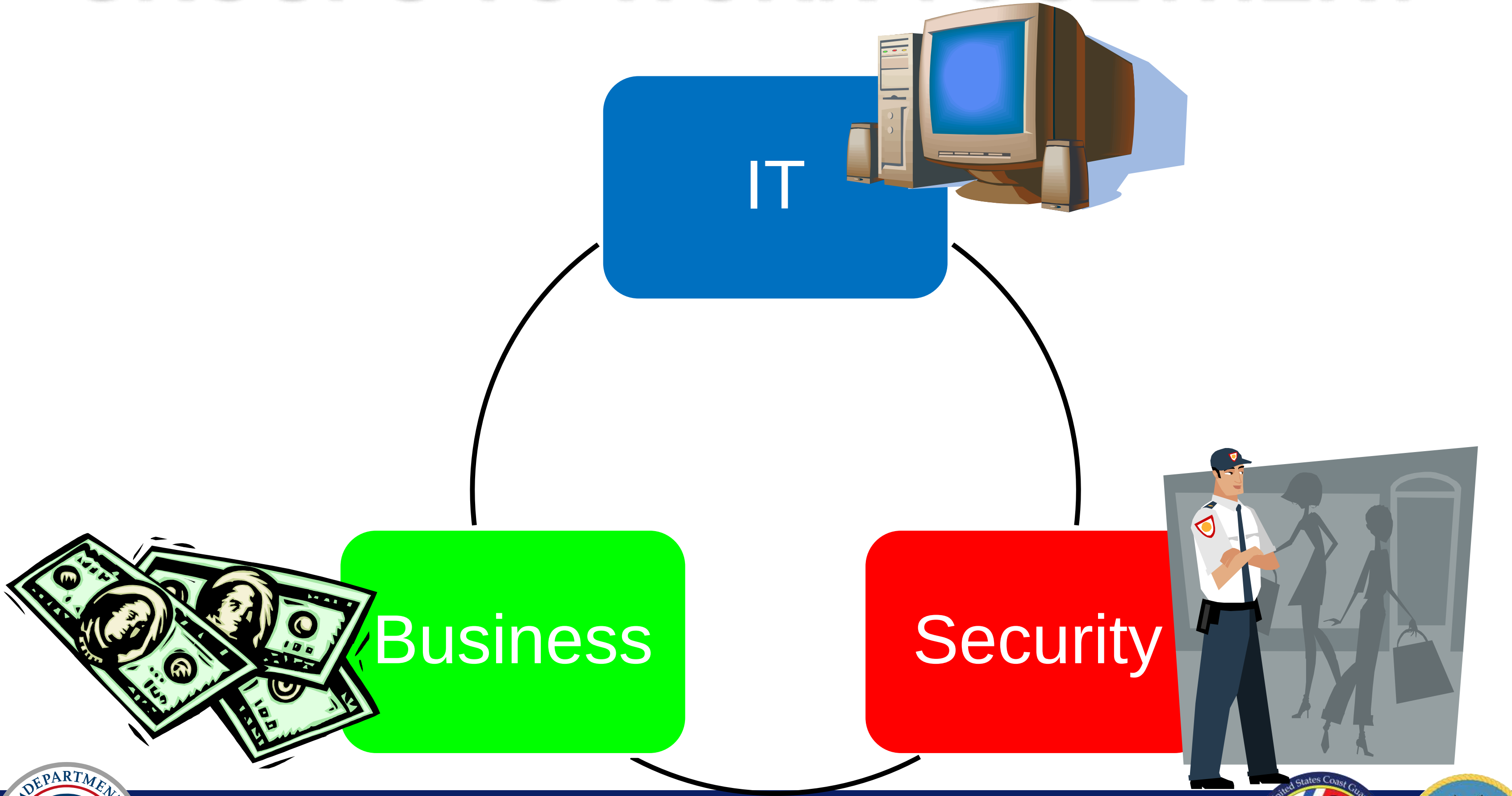
- ❑ FY14 $100 million in federal grant funds were allotted to the PSGP to Group I & Group II ports.
  - Group I ports allotted $47,945,914
  - Group II ports allotted $52,054,086

- ❑ 25 cybersecurity projects were funded in FY14.
  - 23 allotted to public entities
  - 2 allotted to a private company

FY2014 PSGP Cyber Projects Summary

District / Sector or MSU	Group I Port Area	State(s)	Public / Private Entity	Entity	Cybersecurity Project
D11 / SEC LA/LB	Los Angeles/Long Beach	CA	Public	City of Long Beach Harbor Department	Funds allotted for this project includes Cybersecurity Resiliency
	San Francisco Bay	CA	Public	Port of Oakland	Funds allotted for this project includes Cybersecurity Assessment
D5 / SEC Del Bay	Delaware Bay	DE/NJ/PA	Private (MTSA Facility)	Sunoco Logistics Partners, L.P.	Funds allotted for this project includes Cybersecurity Assessment
D8 / SEC NOLA	New Orleans	LA	Public	Plaquemines Port Harbor & Terminal District	Funds allotted for this project includes Cybersecurity Resiliency
			Public	Port of Greater Baton Rouge	Funds allotted for this project includes Cybersecurity Resiliency
			Public	St. Benard Port Harbor & Terminal District	Funds allotted for this project includes Cybersecurity Resiliency
D1 / SEC NY	New York/New Jersey	NY/NJ	Public	County of Nassau, New York	Funds allotted for this project includes Cybersecurity Assessment
D8/ SEC HOU-GAL	Houston - Galveston	TX	Public	Port of Texas City Security Council, Inc.	Funds allotted for this project includes Cybersecurity Assessment

HOW DO WE GET THESE GROUPS TO WORK TOGETHER?



Quote from Rear Admiral Paul Thomas, Assistant Commandant for Prevention Policy

“THERE WERE QUESTIONS FROM THE AUDIENCE ABOUT TIMELINES AND INCENTIVES THAT I’D LIKE TO ADDRESS. THE COAST GUARD JUST RECENTLY CONDUCTED A STUDY ABOUT THE COST BURDEN TO INDUSTRY OF ALL THE REGULATIONS THAT WE HAVE PUBLISHED SINCE 1973. WE FOUND THAT 88% OF THE ENTIRE COST BURDENS OF ALL REGULATIONS, OVER ALL THOSE YEARS, WERE DUE TO TWO REGULATIONS, OPA 90 AND MTSA. BOTH OF THESE REGULATIONS FOLLOWED PREDICTABLE DISASTERS. THE LESSON LEARNED SHOULD BE THAT WE SHOULD NOT WAIT FOR AN INCIDENT TO OCCUR THAT WILL MAKE US MOVE FORWARD ON REACTIVE, MORE EXPENSIVE, REGULATIONS; WE NEED TO BE PROACTIVE IN APPROACHING THIS. WE ARE HERE TO HAVE A DISCUSSION WITH INDUSTRY SO WE CAN DEVELOP A STANDARD TOGETHER, ONE THAT WORKS AND IS REASONABLE IN TERMS OF THE COST BENEFIT. IF WE WAIT UNTIL AN INCIDENT OCCURS, THAT OPPORTUNITY GOES AWAY.”

HTTPS://WWW.YOUTUBE.COM/WATCH?V=RZOVC1ZOUVY&FEATUR EDDED#T=9568

Thank You for your time!

QUESTIONS?