NATIONAL INFRASTRUCTURE ADVISORY COUNCIL (NIAC)

Work Stream #2

CYBER SCOPING STUDY WORKING GROUP

FEBRUARY 16, 2017

- **Mike Wallace,** Former Vice Chairman and COO, Constellation Energy**, Co-Chair**

  Joan McDonald, Principal, JMM Strategic Solutions**, Co-Chair**

  Jan Allman, President, CEO, and General Manager, Marinette Marine Corporation
- **Robert Carr**, Founder and Former Chief Executive Officer, Heartland Payment Systems
- **Ben Fowke,** Chairman and CEO, Xcel Energy
- **Constance Lau,** President and Chief Executive Officer, Hawaiian Electric Industries, Inc.
- **Keith Parker,** General Manager and CEO, Metropolitan Atlanta Rapid Transit Authority

  Beverly Scott, Ph.D., CEO, Beverly Scott Associates, LLC

- ***Work Stream #2***

NATIONAL INFRASTRUCTURE ADVISORY COUNCIL

- Advises the President of the United States on how to ensure the security and resilience of the Nation's 16 critical infrastructures.*
- Comprises 28 CEOs and senior experts from private companies and state and local government who own, operate, and advise on critical infrastructure.
- Charged with strengthening public-private partnerships that can improve security and resilience among the critical infrastructure sectors.
- Issued 270 recommendations in 27 studies since 2001 that have helped to reduce physical and cyber risks to the Nation's infrastructures.

* *Includes energy, transportation, water, communications, banking and finance, chemicals, critical manufacturing, defense industrial base, information technology, nuclear reactors, commercial facilities, dams, healthcare and public health, emergency services, food and agriculture, and government facilities.*

AGENDA

- Executive Summary
- The Cyber Challenge
- Who We Talked to
- What We Found
- How to Proceed
- Special Request to the Council

EXECUTIVE SUMMARY

- Council was tasked to scope a study on cyber risks in critical infrastructure.
- After interviews with senior leaders, classified briefings, and in-depth analysis of recent cyber studies, the Working Group concludes:
  - **Cyber risks to critical infrastructure are severe and urgent action is needed.**
  - **The path we are on will not get us to where we need to be.**
  - **The Nation needs a radically new approach for securing public and private cyber systems.**
  - **NIAC is the most appropriate body to build a new public-private model for achieving national cybersecurity, including a plan for rapid implementation, and present it to the President for approval.**
- We recommend that the Council **request that the President direct NIAC to develop a broad and compelling public-private approach to secure the nation's critical cyber assets.**

KEY SCOPING QUESTIONS

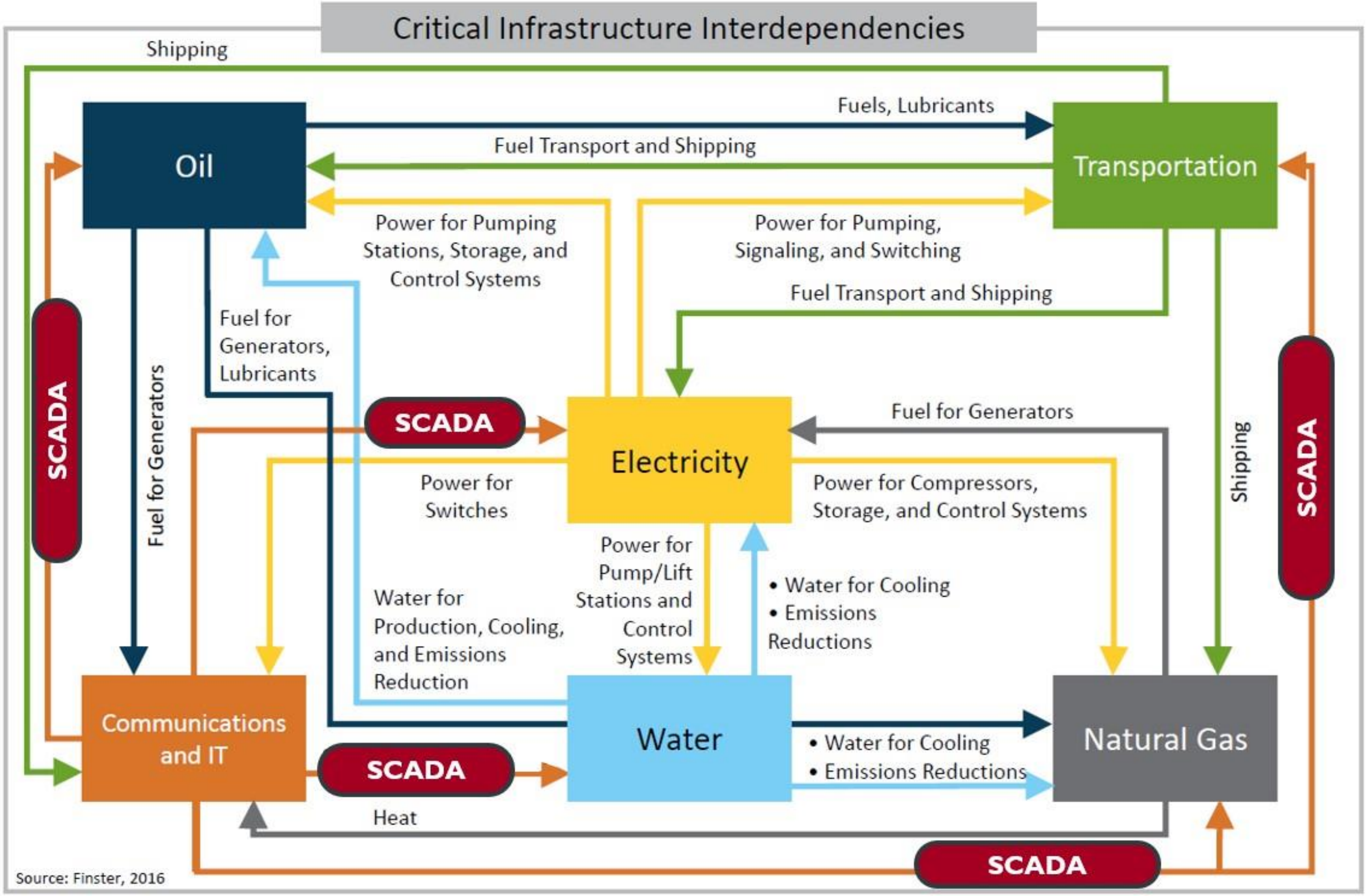
1. What are the most **serious cyber risks** to critical infrastructure?
2. What are the **biggest challenges to reducing these risks**?
3. What are the **roles and responsibilities of the public and private sector** for mitigating cyber risks?
4. What **efforts currently underway** will help reduce cyber risks to critical infrastructure?
5. What are the **gaps in critical infrastructure cybersecurity** that are not being sufficiently addressed?
6. Where can the **NIAC provide the greatest value and leverage** to reduce CI cyber risks for the country?

CYBER RISKS IN CRITICAL INFRASTRUCTURE*

- Cyber risks in critical infrastructure are two-fold:
  - Information and communications technology (**IT**)
  - Operational technologies (including industrial control systems and SCADA systems) (**OT**)
- Cyber attacks on industrial control systems are very serious because they can disrupt vital services, damage critical equipment, threaten human health and safety, and trigger disruptions in other sectors.
- DHS reported 290 cyber attacks on critical infrastructure control systems in 2016. (ICS-CERT)
- DOE concludes that *"the U.S. grid faces imminent danger from cyber attacks, absent a discrete set of actions and clear authorities to inform both responses and threats."*
- Theft of personally identifiable information (PII) and company data is on the rise. Financial institutions experience 300% more cyber attacks than other sectors.
- Internet of Things (IoT) devices, many without strong security, expected to double from 15.4 billion in 2015 to 30.7 billion by 2020.

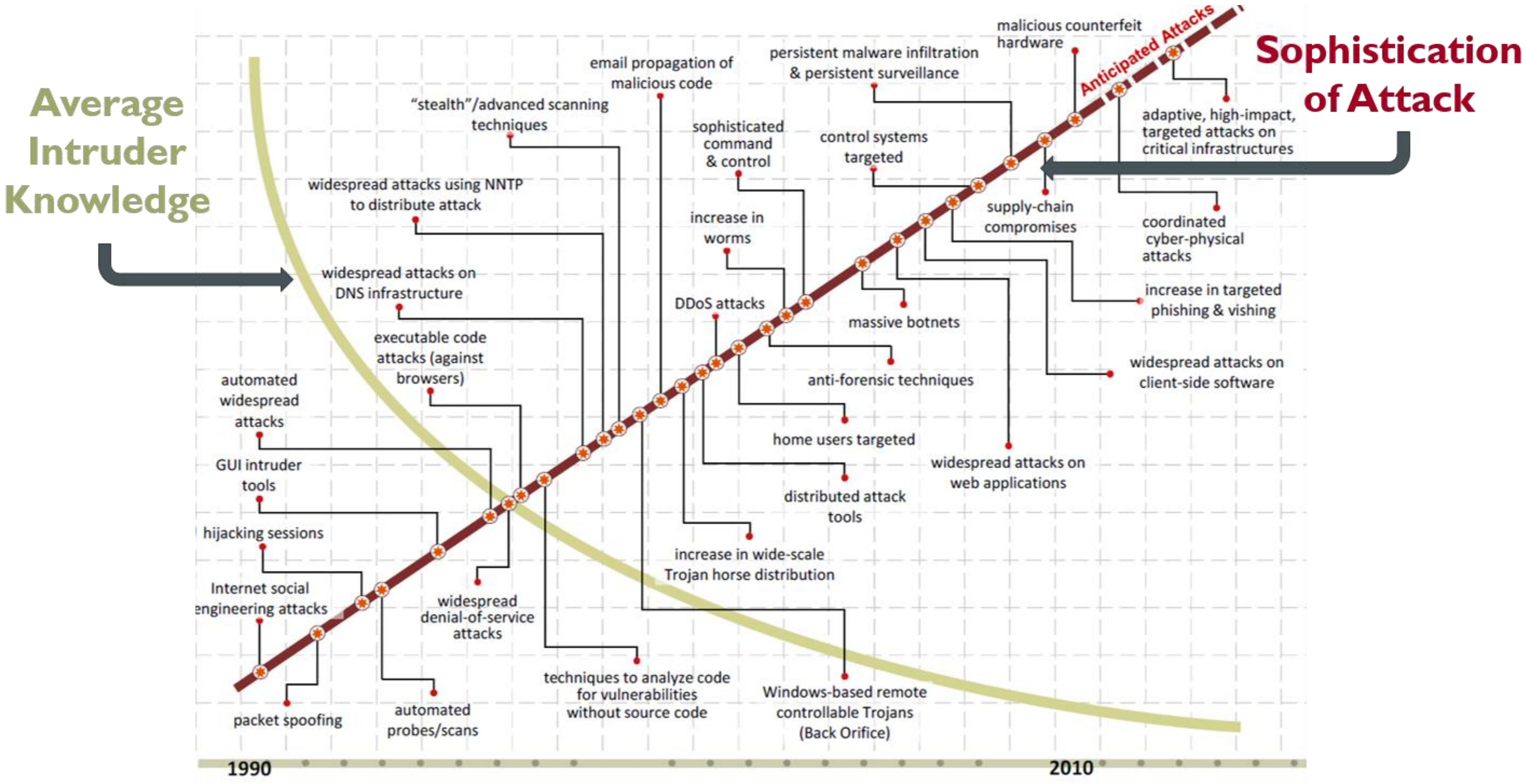
* *Most cyber breaches go undetected or unreported; data on cyber attacks, cyber crime, and cybersecurity are very limited.*

INTERDEPENDENCIES COMPOUND CYBER RISKS


Critical Infrastructure Interdependencies
Shipping
Oil
Fuels, Lubricants
Fuel Transport and Shipping
Transportation
Power for Pumping Stations, Storage, and Control Systems
Power for Pumping, Signaling, and Switching
Fuel Transport and Shipping
Fuel for Generators, Lubricants
SCADA
Fuel for Generators
SCADA
Electricity
Fuel for Generators
Power for Switches
Power for Compressors, Storage, and Control Systems
Shipping
SCADA
Power for Pump/Lift Stations and Control Systems
Water for Production, Cooling, and Emissions Reduction
• Water for Cooling
• Emissions Reductions
Communications and IT
SCADA
Water
• Water for Cooling
• Emissions Reductions
Natural Gas
Heat
SCADA
Source: Finster, 2016

Source: DOE Quadrennial Energy Review 2017

CYBER ATTACKS: MORE SOPHISTICATED, EASIER TO LAUNCH



Source: Software Engineering Institute, Carnegie Mellon University

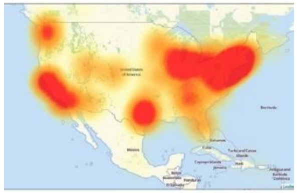
CYBER ATTACKS ON CRITICAL INFRASTRUCTURE

Ukraine Power Grid

December 2015

Electricity Sector

- 225,000 customers lost power
- Military-like planning and execution
- Utilities infiltrated 9 months prior to attack
- Launched with easily available attacks tools



Dyn Attack

October 2016

Multiple Sectors

- Massive botnet DDOS attack involving tens of millions of IP addresses disrupted web traffic
- Compromised ~100,000 insecure IoT devices (webcams, baby monitors, DVRs)
- Caused $110 million in lost revenue and sales

JPMorgan
Chase & Co.

JPMorgan Chase

July 2014

Banking and Finance Sector

- One of the largest data thefts in history
- Compromised data of 83 million accounts
- Cost of breach likely >$1 billion

Shamoon Attacks

January 2017, 2016, 2012

Oil and Natural Gas Sector

- 2017: Weaponized malware hit 15 state bodies and private companies in Saudi Arabia
- 2012: Wiped out 35,000 hard drives of Saudi Aramco causing >$500 million in losses
- Iranian-backed hackers suspected

COST OF CYBER CRIME AND CYBERSECURITY

$500 billion	➢ Global annual business cost of cyber attacks *(Fortune 2015).*
$6 trillion	➢ Projected annual cost of cybercrime in 2021 *(Cybersecurity Ventures 2016).*
$17 million	➢ Estimated average annual cost of cyber crime for U.S. companies in 2016 *(Ponemon 2016).*
$500 million	➢ Annual spending by one U.S. bank to fight cyber crime *(Forbes 2015).*
$1 trillion	➢ Projected cumulative worldwide spending on cybersecurity from 2017 to 2021 *(Cybersecurity Ventures 2016).*
$217	➢ Estimated cost per record of data breach in the U.S. *(Ponemon 2016).*
$19 billion	➢ Projected FY 2017 spending on cybersecurity by the U.S.

The Cyber Challenge

government *(White House 2016).*

DEFINING PUBLIC AND PRIVATE SECTOR ROLES

Security Roles and Responsibilities for Physical and Cyber Risks

Physical Risks

Fed Govt.

↕

Private Sector

- Nuclear Attack
- Natural Disasters
- Active Shooter
- Insider Threats
- Accidents
- Theft and Vandalism

Cyber Risks

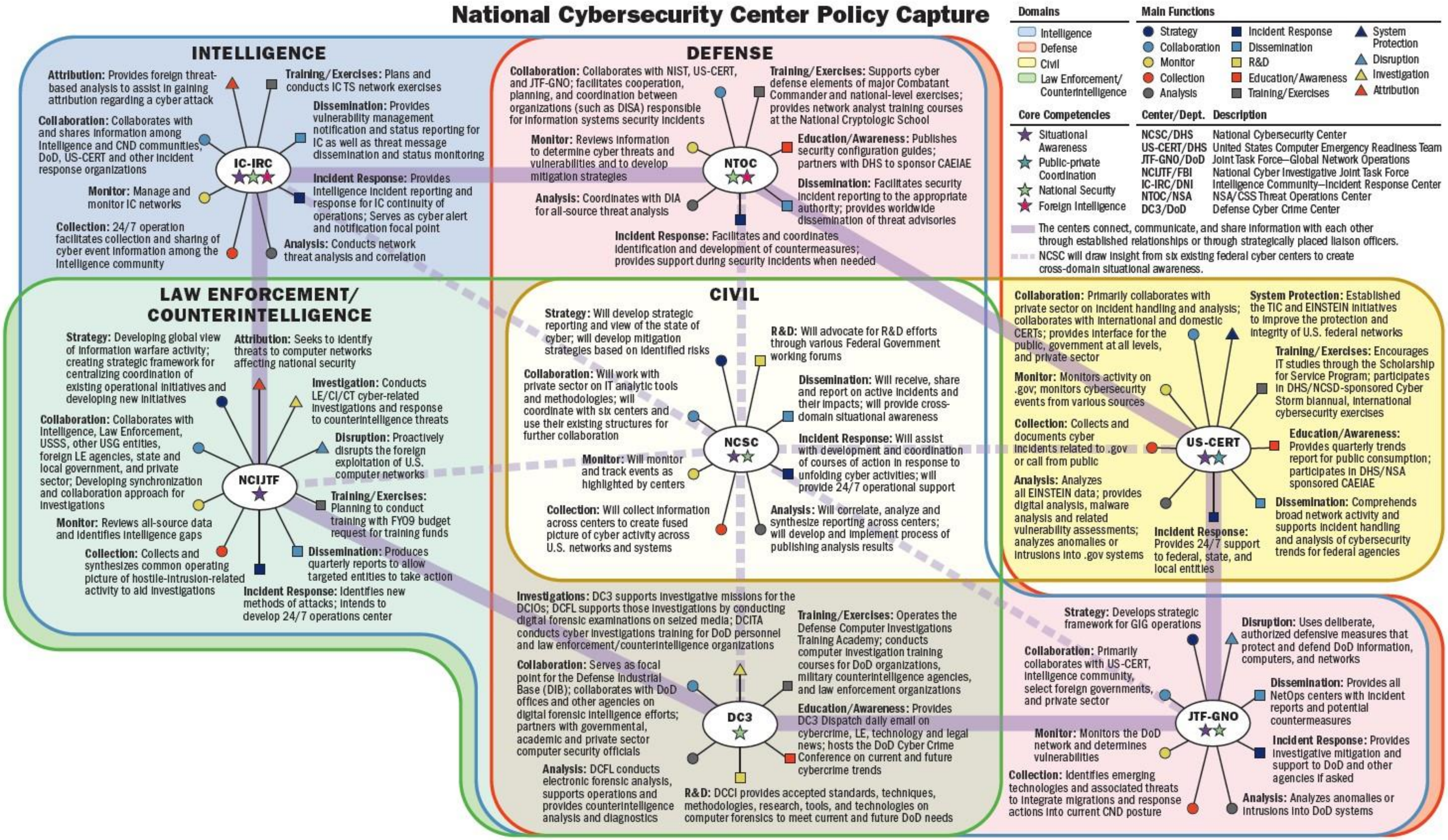
- Nation-State Attack
- Terrorists
- Organized Crime
- Hacktivists
- Script Kiddies
- Accidents

Fed Govt.

↕

Private Sector

"UNTANGLING" FEDERAL CYBERSECURITY RESPONSIBILITIES (2009)



National Cybersecurity Center Policy Capture

Domains

- Intelligence
- Defense
- Civil
- Law Enforcement/ Counterintelligence

Main Functions

- ● Strategy
- ● Collaboration
- ● Monitor
- ● Collection
- ● Analysis
- ■ Incident Response
- ■ Dissemination
- ■ R&D
- ■ Education/Awareness
- ■ Training/Exercises
- ▲ System Protection
- ▲ Disruption
- ▲ Investigation
- ▲ Attribution

Core Competencies

- ★ Situational Awareness
- ★ Public-private Coordination
- ★ National Security
- ★ Foreign Intelligence

Center/Dept.	Description
NCSC/DHS	National Cybersecurity Center
US-CERT/DHS	United States Computer Emergency Readiness Team
JTF-GNO/DoD	Joint Task Force—Global Network Operations
NCIJTF/FBI	National Cyber Investigative Joint Task Force
IC-IRC/DNI	Intelligence Community—Incident Response Center
NTOC/NSA	NSA/CSS Threat Operations Center
DC3/DoD	Defense Cyber Crime Center

The centers connect, communicate, and share information with each other through established relationships or through strategically placed liaison officers.

NCSC will draw insight from six existing federal cyber centers to create cross-domain situational awareness.

INTELLIGENCE

IC-IRC

Attribution: Provides foreign threat-based analysis to assist in gaining attribution regarding a cyber attack

Training/Exercises: Plans and conducts IC TS network exercises

Collaboration: Collaborates with and shares information among Intelligence and CND communities, DoD, US-CERT and other incident response organizations

Dissemination: Provides vulnerability management notification and status reporting for IC as well as threat message dissemination and status monitoring

Monitor: Manage and monitor IC networks

Incident Response: Provides intelligence incident reporting and response for IC continuity of operations; Serves as cyber alert and notification focal point

Collection: 24/7 operation facilitates collection and sharing of cyber event information among the intelligence community

Analysis: Conducts network threat analysis and correlation

DEFENSE

NTOC

Collaboration: Collaborates with NIST, US-CERT, and JTF-GNO; facilitates cooperation, planning, and coordination between organizations (such as DISA) responsible for information systems security incidents

Training/Exercises: Supports cyber defense elements of major Combatant Commander and national-level exercises; provides network analyst training courses at the National Cryptologic School

Monitor: Reviews information to determine cyber threats and vulnerabilities and to develop mitigation strategies

Education/Awareness: Publishes security configuration guides; partners with DHS to sponsor CAEIAE

Analysis: Coordinates with DIA for all-source threat analysis

Dissemination: Facilitates security incident reporting to the appropriate authority; provides worldwide dissemination of threat advisories

Incident Response: Facilitates and coordinates identification and development of countermeasures; provides support during security incidents when needed

LAW ENFORCEMENT/ COUNTERINTELLIGENCE

NCIJTF

Strategy: Developing global view of information warfare activity; creating strategic framework for centralizing coordination of existing operational initiatives and developing new initiatives

Attribution: Seeks to identify threats to computer networks affecting national security

Investigation: Conducts LE/CI/CT cyber-related investigations and response to counterintelligence threats

Collaboration: Collaborates with Intelligence, Law Enforcement, USSS, other USG entities, foreign LE agencies, state and local government, and private sector; Developing synchronization and collaboration approach for investigations

Disruption: Proactively disrupts the foreign exploitation of U.S. computer networks

Training/Exercises: Planning to conduct training with FY09 budget request for training funds

Monitor: Reviews all-source data and identifies intelligence gaps

Collection: Collects and synthesizes common operating picture of hostile-intrusion-related activity to aid investigations

Dissemination: Produces quarterly reports to allow targeted entities to take action

Incident Response: Identifies new methods of attacks; intends to develop 24/7 operations center

CIVIL

NCSC

Strategy: Will develop strategic reporting and view of the state of cyber; will develop mitigation strategies based on identified risks

R&D: Will advocate for R&D efforts through various Federal Government working forums

Collaboration: Will work with private sector on IT analytic tools and methodologies; will coordinate with six centers and use their existing structures for further collaboration

Dissemination: Will receive, share and report on active incidents and their impacts; will provide cross-domain situational awareness

Incident Response: Will assist with development and coordination of courses of action in response to unfolding cyber activities; will provide 24/7 operational support

Monitor: Will monitor and track events as highlighted by centers

Collection: Will collect information across centers to create fused picture of cyber activity across U.S. networks and systems

Analysis: Will correlate, analyze and synthesize reporting across centers; will develop and implement process of publishing analysis results

US-CERT

Collaboration: Primarily collaborates with private sector on incident handling and analysis; collaborates with international and domestic CERTs; provides interface for the public, government at all levels, and private sector

System Protection: Established the TIC and EINSTEIN initiatives to improve the protection and integrity of U.S. federal networks

Training/Exercises: Encourages IT studies through the Scholarship for Service Program; participates in DHS/NCSD-sponsored Cyber Storm biannual, international cybersecurity exercises

Monitor: Monitors activity on .gov; monitors cybersecurity events from various sources

Collection: Collects and documents cyber incidents related to .gov or call from public

Education/Awareness: Provides quarterly trends report for public consumption; participates in DHS/NSA sponsored CAEIAE

Analysis: Analyzes all EINSTEIN data; provides digital analysis, malware analysis and related vulnerability assessments; analyzes anomalies or intrusions into .gov systems

Incident Response: Provides 24/7 support to federal, state, and local entities

Dissemination: Comprehends broad network activity and supports incident handling and analysis of cybersecurity trends for federal agencies

DC3

Investigations: DC3 supports investigative missions for the DCIOs; DCFL supports those investigations by conducting digital forensic examinations on seized media; DCITA conducts cyber investigations training for DoD personnel and law enforcement/counterintelligence organizations

Training/Exercises: Operates the Defense Computer Investigations Training Academy; conducts computer investigation training courses for DoD organizations, military counterintelligence agencies, and law enforcement organizations

Collaboration: Serves as focal point for the Defense Industrial Base (DIB); collaborates with DoD offices and other agencies on digital forensic intelligence efforts; partners with governmental, academic and private sector computer security officials

Education/Awareness: Provides DC3 Dispatch daily email on cybercrime, LE, technology and legal news; hosts the DoD Cyber Crime Conference on current and future cybercrime trends

Analysis: DCFL conducts electronic forensic analysis, supports operations and provides counterintelligence analysis and diagnostics

R&D: DCCI provides accepted standards, techniques, methodologies, research, tools, and technologies on computer forensics to meet current and future DoD needs

JTF-GNO

Strategy: Develops strategic framework for GIG operations

Disruption: Uses deliberate, authorized defensive measures that protect and defend DoD information, computers, and networks

Collaboration: Primarily collaborates with US-CERT, intelligence community, select foreign governments, and private sector

Dissemination: Provides all NetOps centers with incident reports and potential countermeasures

Monitor: Monitors the DoD network and determines vulnerabilities

Incident Response: Provides investigative mitigation and support to DoD and other agencies if asked

Collection: Identifies emerging technologies and associated threats to integrate migrations and response actions into current CND posture

Analysis: Analyzes anomalies or intrusions into DoD systems

Source: https://www.whitehouse.gov/files/documents/cyber/CybersecurityCentersGraphic.pdf, accessed December 2016 (now removed)

CYBER CHALLENGE: KEY TAKEAWAYS

- Cyber risks to critical infrastructure are extensive and urgent
- Attackers have the advantage and their capabilities increasingly outpace our defenses.
- There is no clear national strategy or accountability that indicates who is responsible to defend the collective entities in the Nation against cyber attacks
- Both public and private capabilities and resources are needed to reduce cyber risks to critical infrastructure
- Quick, bold, and decisive action is needed that builds on a foundation of strong public-private partnership

INTERVIEWS

National Security Council Staff

- **Stephanie Morrison**, Director, Critical Infrastructure Policy
- **Monica Maher**, Director, Cybersecurity
- **Asha Tribble**, former NSC Staff
- **Darrell Darnell**, former NSC staff

Intelligence Community

- **Richard Ledgett**, Deputy Director, NSA
- **Glenn Gerstell**, General Counsel, NSA; former NIAC member
- **Lt. Gen Kevin McLaughlin**, Deputy Commander, US Cyber Command
- **Gen. Keith Alexander (ret.),** former Director, NSA; former Commander, US Cyber Command
- **Richard Danzig**, Chairman, Center for a New American Security; Senior Fellow, Johns Hopkins Applied Physics Lab; former Secretary of the Navy

INTERVIEWS

Critical Infrastructure Community

- **Tom Fanning,** Chairman and CEO, Southern Company; Chair, Electricity SCC
- **Alfred Berkeley,** former President and Vice-Chairman, NASDAQ; former NIAC member
- **Scott Aaronson**, Executive Director, Security and Business Continuity, Edison Electric Institute
- **Bill Nelson**, President and CEO, Financial Services Information Sharing and Analysis Center

Government Leaders in Critical Infrastructure

- **Caitlin Durkovich**, Assistant Secretary, Infrastructure Protection, DHS
- **Pat Hoffman**, Assistant Secretary, Electricity Delivery and Energy Reliability, DOE
- **Paul Stockton**, Managing Director, Sonecon; Senior Fellow, Johns Hopkins Applied Physics Lab; former Assistant Secretary for Homeland Defense, DOD
- **Col. Bob Stephan** (Ret.), USAF, former Assistant Secretary, Infrastructure Protection, DHS
- **Jim Caverly,** former Director, Partnership and Outreach Division, DHS
- **Brian Peretti**, Financial Services Critical Infrastructure Program Manager, US Treasury
- **Eric Goldstein**, Senior Counselor to the Under Secretary of the National Protection and Programs Directorate (NPPD), DHS
- **Richard Moore**, Associate Director for Security Policy and Plans, DOT; former Branch Chief, DHS Office of Cyber and Infrastructure Analysis

BRIEFINGS AND PANEL DISCUSSIONS

- National Security Agency (NSA) [classified]
- NSA and US Cyber Command [classified and unclassified]
- Office of the Director of National Intelligence (ODNI) [classified]
- Cybersecurity Emergency Response Team (US-CERT) [classified]
- Mike Assante, SANS Institute – Ukrainian Cyber Attack [unclassified]
- Financial Sector Coordinating Council [unclassified]
- Draper Laboratory [unclassified]
- Federal Bureau of Investigation (FBI) [unclassified]

SELECTED CYBER STUDIES AND STRATEGIES

- Commission on Enhancing National Cybersecurity. ***Report on Securing and Growing the Digital Economy***, 2016.
- Bipartisan Policy Center. ***Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat,*** 2014.
- ***Roadmaps to Secure Control Systems*** (Energy, Chemical, Water, Dams, Transportation), 2006-2011.
- National Institute of Standards and Technology. ***Framework for Improving Critical Infrastructure Cybersecurity,*** 2014.
- U.S. Department of Homeland Security. ***Strategic Principles for Securing the Internet of Things, (IoT),*** 2016.
- U.S. Department of Homeland Security. ***The National Cyber Incident Response Plan*** (Review Draft), 2016.
- U.S. Department of Defense. ***The DOD Cyber Strategy***, 2015.
- Defense Science Board. ***Resilient Military Systems and the Advanced Cyber Threat***, 2013.
- UK Government Communications Headquarters. ***National Cyber Security Strategy 2016-2021***, 2016.
- Homeland Security Advisory Council, Cybersecurity Subcommittee. ***Final Report, Part I – Incident Response***, 2016.
- The President's Review Group on Intelligence and Communications Technologies. ***Liberty and Security in a Changing World, Report and Recommendations***, 2013.
- The White House. ***Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure***, 2009.
- The White House. ***Federal Cybersecurity Research and Development Strategic Plan***, *2016*.
- The White House. ***Federal Cybersecurity Workforce Strategy***, 2016.

FINDINGS

1. **Our ability to defend private sector cyber networks is not keeping up with the threat.**
   - ➢ Critical infrastructure owners and operators are not doing enough to protect their cyber systems from risks.
   - ➢ Industrial control systems (ICS) connected to business IT systems and the internet constitute a *systemic cyber risk* among critical infrastructures.
2. **Cybersecurity of critical infrastructure is a shared responsibility that needs effective public-private partnership to drive joint action.**
   - ➢ Federal and private sector resources are not organized effectively to help the private sector secure their critical cyber systems.
   - ➢ Information sharing has improved, but still has persistent flaws.
3. **Government efforts over the past 30 years have fallen short in reducing cyber risks in critical infrastructure sectors.**
   - ➢ Multiple entities are responsible for various aspects of cybersecurity but the country lacks an integrated, focused approach to defend the Nation.
   - ➢ Cyber legislation, regulations, and executive actions are inadequate for motivating private action to improve cybersecurity.
   - ➢ Alternative national models for cybersecurity offer promising new approaches.

Finding 1: Our Ability to Defend Private Sector Cyber Networks Is Not Keeping Up with the Threat.

In today's world, attackers have the advantage. The right adversary with the right capabilities and intent can breach just about any system. Rather than react to the latest threat, we must anticipate future trendlines and design systems to defeat them.

A. Critical infrastructure owners and operators are not doing enough to protect their cyber systems from risks.

Many companies are not practicing basic cyber hygiene despite the availability of effective tools and practices. Managers often do not fully understand the magnitude or complexity of the risks they face. There is also little incentive to improve cybersecurity in competitive environments.

B. Industrial control systems (ICS) connected to business IT systems and the internet constitute a *systemic cyber risk* among critical infrastructures.

Automated, cyber-based control systems improve productivity but also introduce new cyber risks. Interconnected cyber systems within supply chains and across infrastructures means that an ICS cyber breach can cascade to connected systems and cause physical damage and threaten human health and safety. Securing these systems should be a national priority.

Finding 2: Cybersecurity of Critical Infrastructure Is a Shared Responsibility that Needs Effective Public-Private Partnership to Drive Joint Action.

Growing dependence by government, businesses, and communities on critical services means that an attack on critical infrastructure is an attack on civil society. Defense against well-resourced adversaries requires the collective resources of the public and private sectors. This is a national risk management problem that must be addressed at the highest executive levels.

A. Federal and private sector resources are not organized effectively to help the private sector secure their critical cyber systems.

Gaps and overlaps in the cybersecurity authorities, missions, roles, and responsibilities of government departments and agencies is inefficient and precarious; a bold new approach is needed. The public and private sectors must compete for a limited pool of highly trained cyber experts, creating a shortage of cybersecurity leadership and expertise.

B. Information sharing has improved, but still has persistent flaws.

Intelligence information now being shared with the private sector is not well organized. Successful information sharing requires bi-directional flows that allow for machine-to-machine mitigations. Yet companies are reluctant to use automated services that provide immediate response to cyber attacks due to a lack of trust in government information protection.

Finding 3: Government Efforts Over the Past 30 Years Have Fallen Short in Reducing Cyber Risks in Critical Infrastructure Sectors.

Progress in cybersecurity technologies and policies have not kept pace with rising cyber risks. We have created a patchwork of legislation, policies, and approaches, but lack a cohesive national strategy.

A. **Multiple entities are responsible for various aspects of cybersecurity but the country lacks an integrated, focused approach to defend the Nation.**

- ➢ We lack a cohesive framework for cyber defense and our response to a large-scale physical-cyber attack on critical infrastructures today is likely to be inefficient.

B. **Cyber Legislation, Regulations, and Executive Actions Are Inadequate for Motivating Private Action to Improve Cybersecurity.**

- ➢ Legislation and policy directives are often blunt tools for cybersecurity. Their slow development lags rapidly changing cyber risks. Unintended consequences can also impede beneficial security efforts. Market-driven approaches with appropriate incentives provides a faster and more flexible way to drive private sector security actions.

C. **Alternative national models for cybersecurity offer promising new approaches.**

- ➢ The governments of Israel, UK, and others use novel approaches to mitigate private sector cyber risks. However, their viability within the United States must take into account the large scale and digital footprint of U.S. infrastructure.

THREE URGENT CYBER PRIORITIES

1. **Triage Today's Problems**
   - ➢ Implement immediate and urgent fixes to address the most serious cyber risks to critical infrastructure. Focus on the sectors and set of assets that, if compromised, would result in major economic, safety, and security consequences to the U.S.
   - ➢ Improve cyber hygiene across all critical infrastructures and consider some form of compliance.
   - ➢ Improve information sharing mechanisms, leading to machine-to-machine exchanges
2. **Develop Novel Approaches for Cyber Resilience**
   - ➢ Design next-generation cyber systems that are inherently secure, resilient, and self-healing, particularly those that control critical functions. Develop solutions that make it extremely difficult and economically unattractive to extract value.
3. **Strengthen Public-Private Partnership and Leadership**
   1. Develop effective executive-level, public-private mechanisms to strengthen leadership and efficient decisionmaking concerning critical cyber incidents and policy actions.
   2. Streamline, reconfigure, and clarify roles and responsibilities within the federal government

HOW TO PROCEED

- **The path we are on will not get us to where we need to be.** A bold, new, integrated and comprehensive approach is needed to direct the country's cybersecurity needs based on a new model and level of public-private partnership.
- NIAC—the President's cross-sector, senior executive advisors on critical infrastructure—should undertake the development of the framework, structure, authorities, and public and private roles needed to build a new public-private approach to cybersecurity for critical infrastructure.
- Our approach to national cybersecurity must:
  1. Be significantly more impactful and robust, with very specific recommendations for the President for new structures, authorities, roles, responsibilities, staffing, and resource commitments.
  2. Engage senior leaders and key stakeholders to solicit the best ideas.
  3. Address immediate needs and anticipate future needs.
- The Council should ***accelerate*** the launch of the cyber study with a letter to the President.

CYBER STUDY DESIGN

Phase 1: Frame out the proposed public-private model for achieving national cybersecurity.

- Build on the tremendous foundation of previous councils and commissions.
- Propose a new strawman structure, framework, and approach for cybersecurity.

Phase 2: Solicit input from the nation's top leaders and experts to strengthen the model.

- Conduct a series of engagements with the best and brightest experts to develop the features, characteristics, authorities, structure, staffing, governance, leadership, priorities, and resource requirements for this new model.
- Challenge the model, shape it, and improve it.

Phase 3: Refine and recommend a comprehensive national cybersecurity model and execution plan to the POTUS.

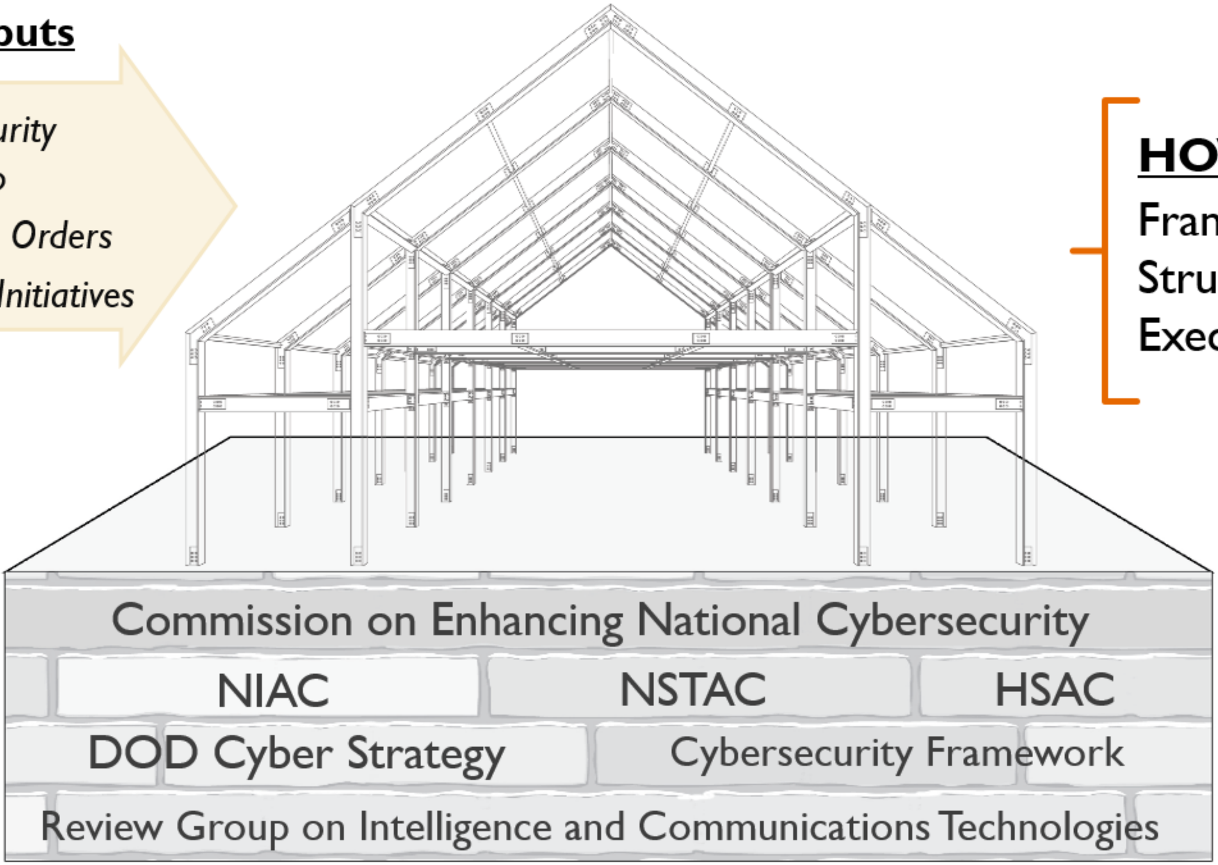
- Recommend a comprehensive approach to direct actions that will provide the speed, focus, and effectiveness to leverage a public-private partnership for the security of the nation's cyber assets, and the critical components these assets control.

NIAC WILL BUILD ON RECENT CYBER STRATEGIES

Proposed NIAC Cyber Study

Dynamic Inputs

- *WH Cybersecurity Advisory Group*
- *New Executive Orders*
- *Congressional Initiatives*



Commission on Enhancing National Cybersecurity

NIAC

NSTAC

HSAC

DOD Cyber Strategy

Cybersecurity Framework

Review Group on Intelligence and Communications Technologies

HOW

Framework, Structure, & Execution Plan

WHAT

Cyber Challenges & Solutions

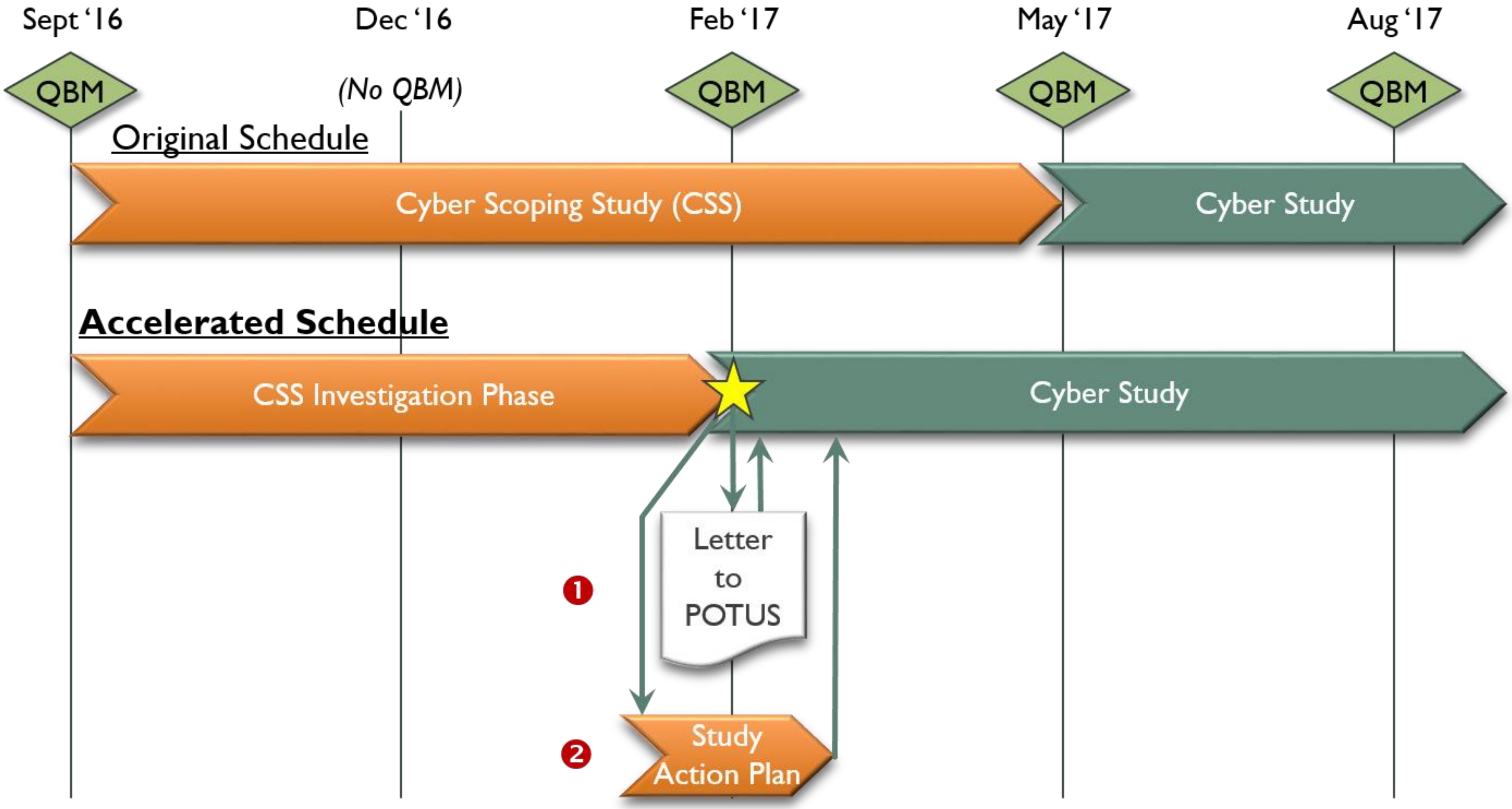
SPECIAL REQUEST TO THE COUNCIL

1. Prepare a letter to the President recommending that he direct the Council to immediately begin working with stakeholders on the "new Cyber Study" to develop the framework, structure, public and private roles, and authorities needed to build a new public-private approach to cybersecurity for critical infrastructure that is significantly more impactful and robust.

2. Approve the Working Group's recommendation to end the investigative portion of Cyber Scoping Study and begin work at once to prepare a detailed action plan for the "new Cyber Study" to allow rapid startup once approval is received.

3. Request that the Administration increase staff funding and resources commensurate with the scope, timing, and importance of the cyber study.

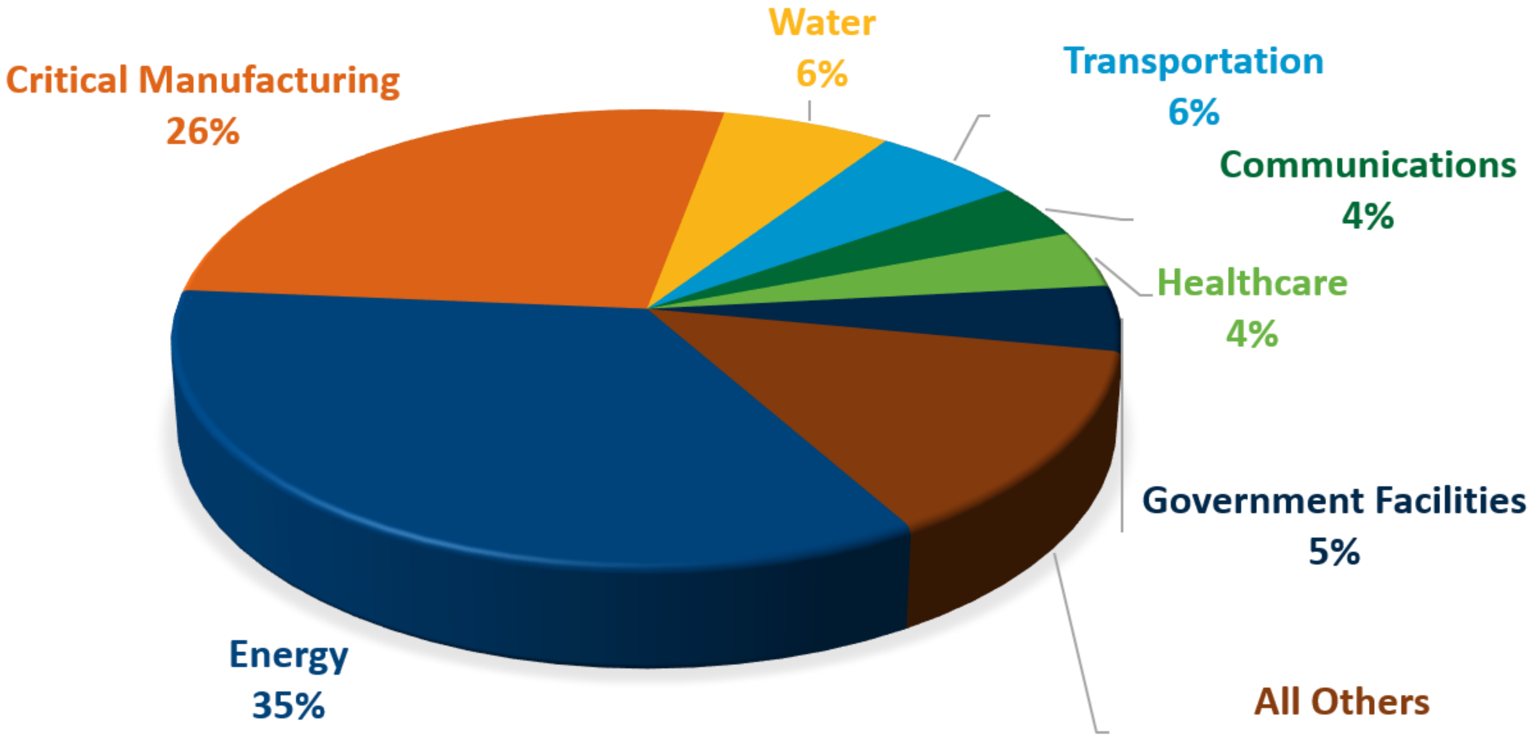
CYBER SCOPING STUDY PROCESS



APPENDIX

CYBER ATTACKS ON CRITICAL INFRASTRUCTURE

Cyber Incidents Against Critical Infrastructures Reported to ICS-CERT (2013-2015)*

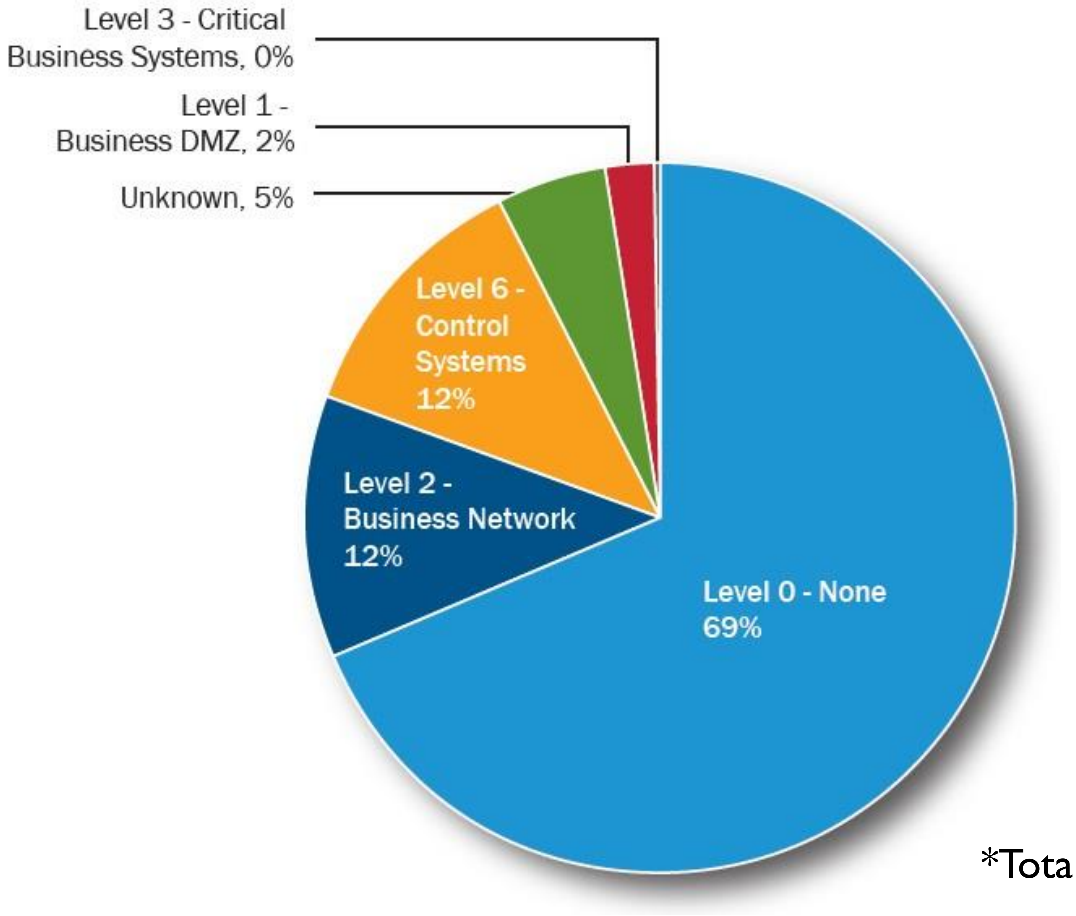


*Total incidents: 796

Source: ICS-CERT Monitors

DEPTH OF CYBER INTRUSION

Observed Depth of Intrusion into Critical Infrastructure (FY 2015)*



*Total incidents: 295

Source: ICS-CERT

CYBERSECURITY CONSIDERATIONS IN CRITICAL INFRASTRUCTURES (OT vs. IT)

Operational Technology (OT)/ Industrial Control Systems (ICS) ≠ ***Business IT Systems***

- Compromise of OT can disable operations, disrupt critical services to customers, and damage highly specialized equipment.
- OT must be able to survive a cyber incident while sustaining critical functions. Real-time operations are imperative; latency is unacceptable.
- Many OT systems must operate 24/7 with high reliability and availability; no down time for patching/upgrades.
- Some OT components do not have enough computing resources to support additional cybersecurity capabilities.
- OT components may be widely dispersed and located in publicly accessible areas where they are subject to physical tampering.
- OT order of priorities: Availability, Integrity, Confidentiality (AIC); IT order of priorities: Confidentiality, Integrity, Availability (CIA)

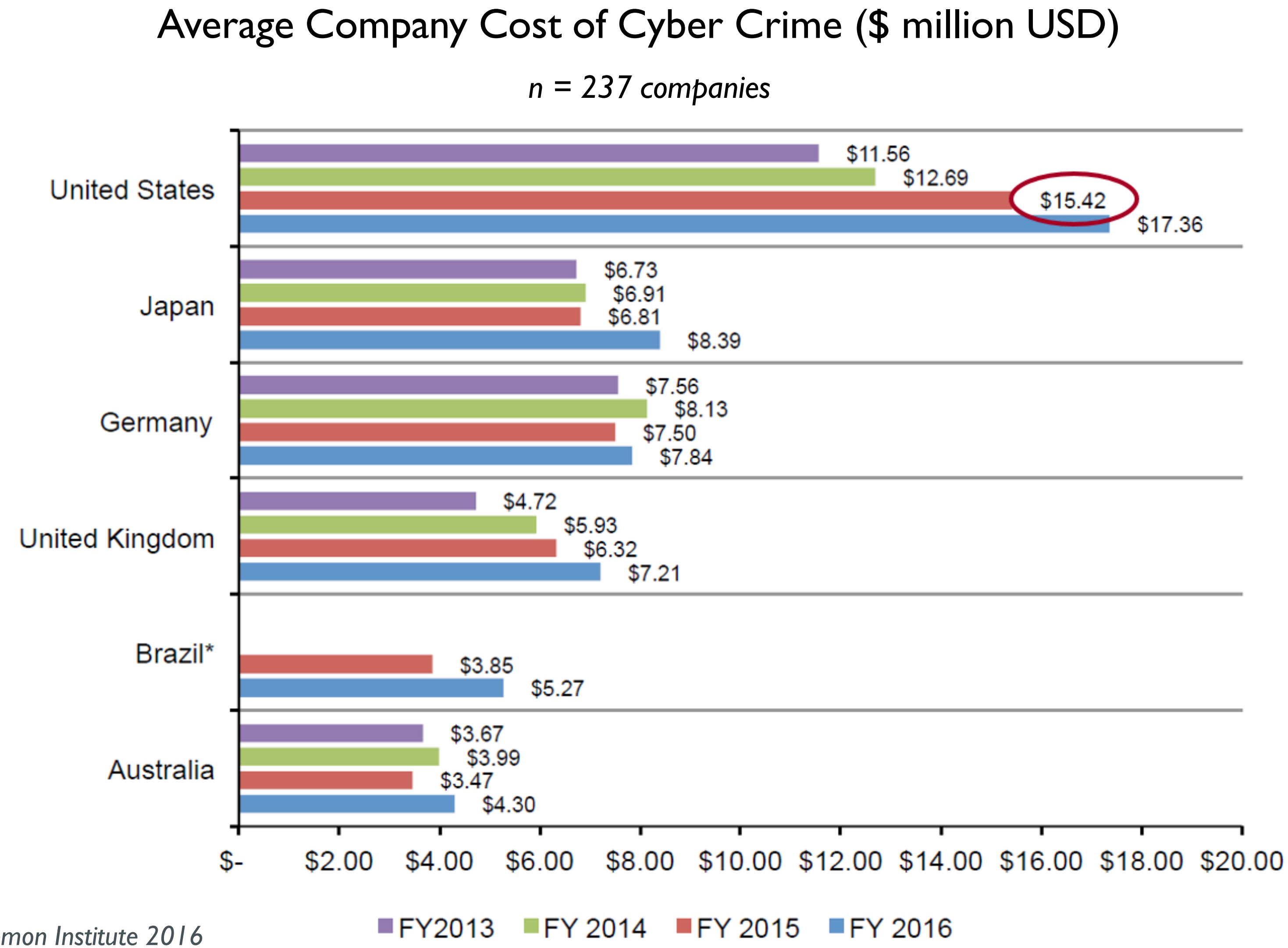
RECENT BREACHES INVOLVING PRIVACY, PII, IP

Incident	Date	Sector(s) Affected	US / Foreign	Likely Source/Attacker	Privacy/PII Impacts
SWIFT attacks	February 2016	**Financial Services**	Foreign	Criminal Hackers, Insiders involved	Attempt to transfer $951M from transferred; other banks hit
OPM Hacks	April & May	**Government Facilities**	US	Nation-State: China	Many different kinds of PII stolen: security clearance information, personal information, finger prints of all Federal employees
Home Depot Breach	September 2014	**Financial Services**	US	Criminal Hackers via 3rd party vendor	56 million credit and debit cards in the U.S. and Canada compromised.
Alcoa spear phishing	May 2014	**Critical Manufacturing**	US	Nation-State: China	PII from company executives potentially exposed. Stolen intellectual property beneficial to
Target Breach	March 2014	**Financial Services**	US	Criminal Hackers via 3rd party vendor	70 million accounts including PII debit cards compromised

RECENT BREACHES INVOLVING ICS, IOT

Incident	Date	Sector(s) Affected	US / Foreign	Likely Source/Attacker	Critical infrastructure impacts
Dyn attack	October 2016	**Communications Financial Services, IT**	US	Hacktivist/unknown	Major Communications and Financial Services company sites (Comcast, Verizon, PayPal, Visa) and services down or slow. Millions of IoT devices
Ukraine / BlackEnergy	December 2015	**Energy**	Foreign	Nation-State: Russia	SCADA vulnerabilities revealed, substations had to be manually controlled. Many US substations don't have manual backup systems.
German steel mill	January 2015	**Critical Manufacturing**	Foreign	Probable Nation State/unknown	“Massive” physical damage to critical be shut down
National Inventory of Dams	May 2013	**Dams**	US	Chinese origin, possible Nation-State	Sensitive information on 79,000 dams included
Saudi Aramco / Shamoon	August 2012	**Energy**	Foreign	Nation-State: Iran	Internal business operations severely disrupted for days; oil production proceeded with no impact to ICS systems due to quick action by the company
U.S. Pipelines	March 2012	**Energy**	US	APT (nation state), possibly China	6-month campaign breached 20+ companies and exfiltrated data on the ICS/SCADA environment
Stuxnet	July 2010	**Energy**	Foreign	Nation-State: U.S./Israel (not confirmed)	Severe damage to centrifuge equipment that were operated well out of safe bounds

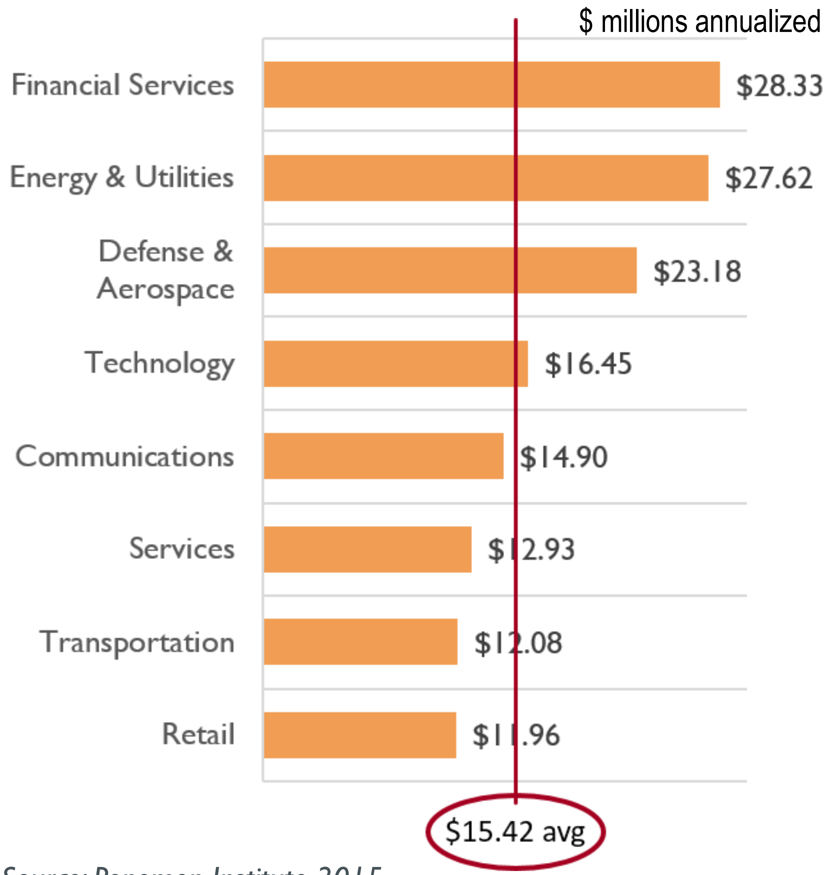
ESTIMATED COST OF CYBER CRIME



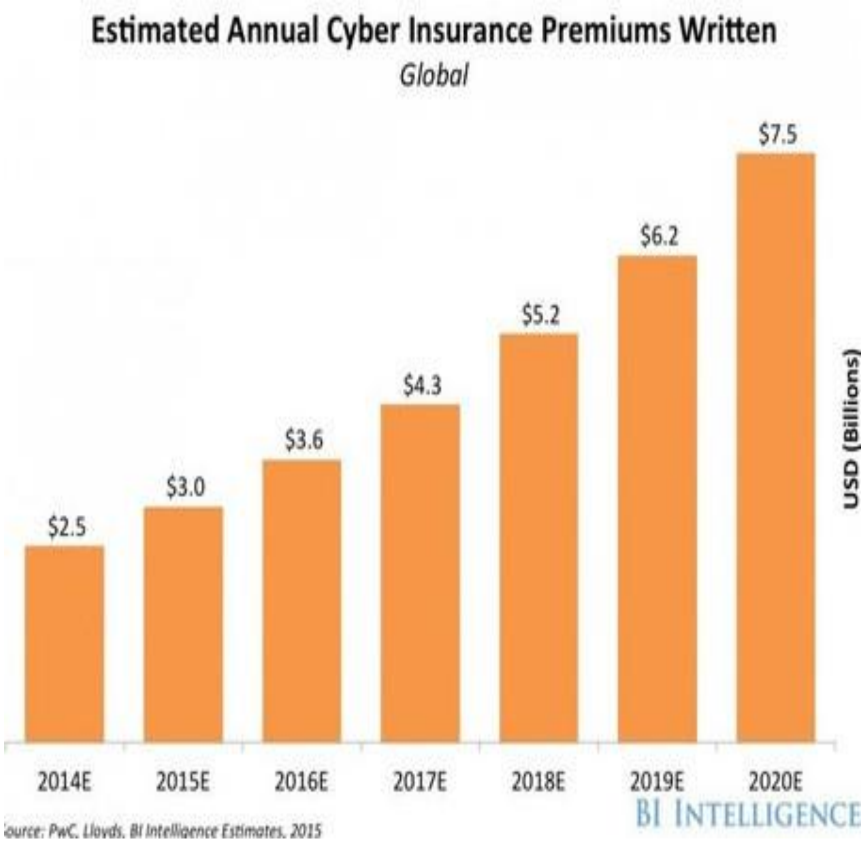
Source: Ponemon Institute 2016

THE COST OF CYBERSECURITY

Average US Company Cost of Cyber Crime by Industry Sector in 2015



Source: Ponemon Institute 2015


Estimated Annual Cyber Insurance Premiums Written

Global

ource: PwC, Lloyds, BI Intelligence Estimates, 2015

OVERVIEW OF FEDERAL EFFORTS

1. Federal Coordination Plans and Strategies
2. Federal Cyber Commissions and Councils
3. Government Cyber Coordination Groups
4. Cyber Legislation, Regulations, Executive Actions, and Policies

FEDERAL COORDINATION PLANS AND STRATEGIES

1. Cybersecurity National Action Plan (2016)
2. Federal Cybersecurity Research and Development Strategic Plan (2016)
3. Federal Cybersecurity Workforce Strategy (2016)
4. DOD Cyber Strategy (2015)
5. The National Cyber Incident Response Plan (2016)

FEDERAL CYBER COMMISSIONS AND COUNCILS

1. Commission on Enhancing National Cybersecurity (CENC), *Report on Securing and Growing the Digital Economy, December 2016*
2. White House, *Joint United States-Canada Electric Grid Security and Resilience Strategy, December 2016*
3. Homeland Security Advisory Council, Cybersecurity Subcommittee, *Report on Incident Response, June 2016*
4. National Security Telecommunications Advisory Committee (NSTAC), *Report on the Internet of Things, November 2014*
5. The President's Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World, December 2013*

➢ *New White House Cybersecurity Advisory Group (2017)*

COMMISSION ON ENHANCING NATIONAL CYBERSECURITY (CENC) – BACKGROUND

- Created by Executive Order 13718 on February 9, 2016
- 12 Commissioners from industry, academia, and former government
- Supported by 6 full-time staff and $5.5 million.
- Charge:
  - ➢ Make detailed recommendations to strengthen cybersecurity in both the public and private sectors . . . and bolster partnerships between Federal, State, and local government and the private sector
  - ➢ Support the development, promotion, and use of cybersecurity technologies, policies, and best practices
  - ➢ Address actions that can be taken over the next decade
- Critical Infrastructure – one of eight topics studied, *and was the most cited topic for Commission consideration in public responses (50% respondents were companies)*
- 6 Imperatives, 16 Recommendations, 52 Actions

CENC: IMPERATIVES

1. Protect, defend, and secure today's information infrastructure and digital networks.

2. Innovate and accelerate investment for the security and growth of digital networks and the digital economy.

3. Prepare consumers to thrive in a digital age.

4. Build cybersecurity workforce capabilities.

5. Better equip government to function effectively and securely in the digital age.

6. Ensure an open, fair, competitive, and secure global digital economy.

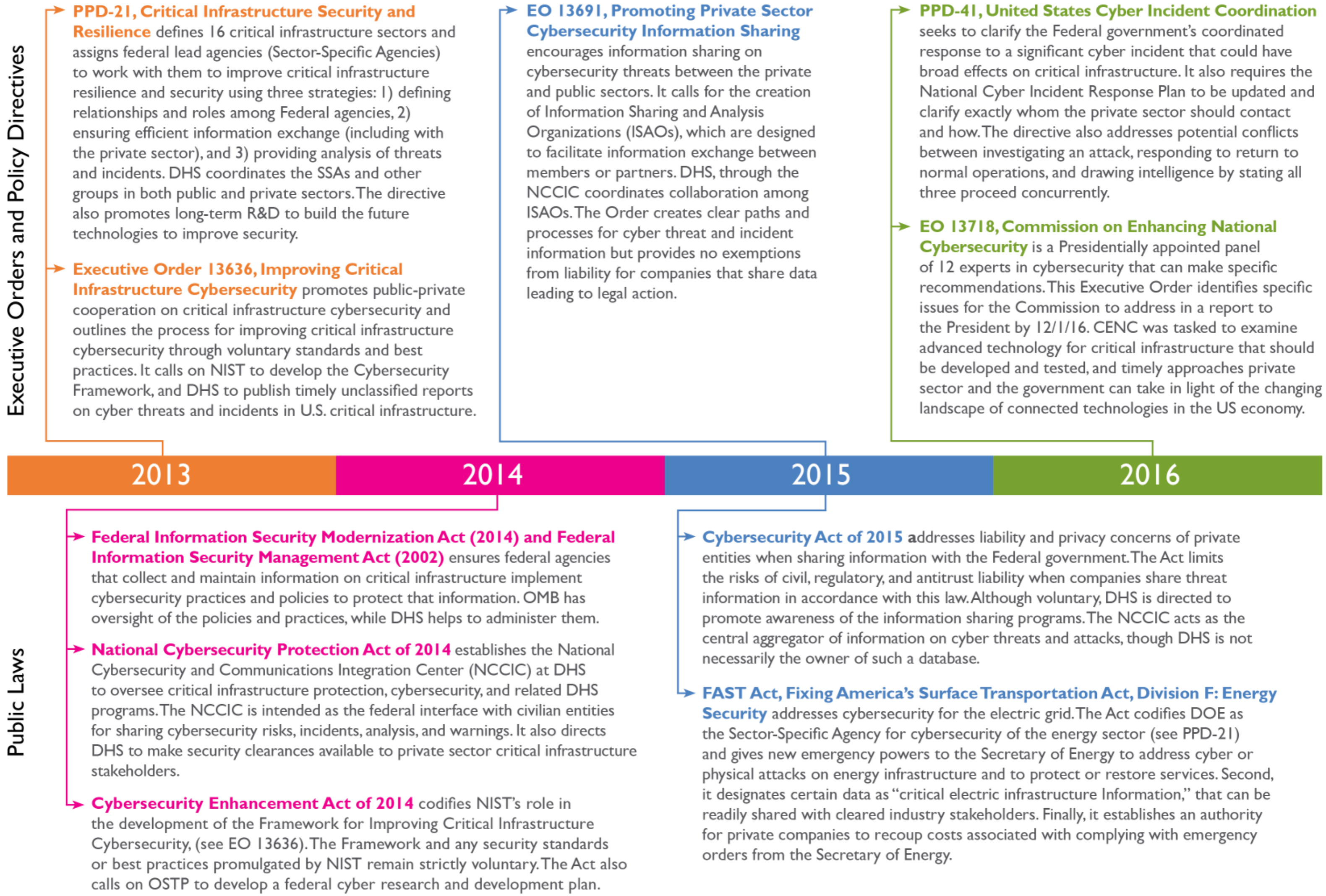
CENC: NOTABLE RECOMMENDATIONS

- Recommendation 1.1: The private sector and the Administration should collaborate on a roadmap for improving security of digital networks
- Recommendation 1.2: Physical-cyber convergence: work closely with the private sector to define and implement a new model for how to defend and secure critical infrastructure
- Recommendation 2.2: Make the development of usable, affordable, inherently secure, and resilient/recoverable systems a top R&D priority
- Recommendation 4.2: Proactively address workforce gaps through capacity building while investing in innovations (e.g. automation, machine learning, and artificial intelligence) that will redistribute this workforce
- Recommendation 5.4: Better match cybersecurity responsibilities with the structure and positions in the executive office
- Recommendation 5.5: Clarify cybersecurity mission responsibilities across departments and agencies

GOVERNMENT COORDINATION GROUPS

1. FBI Field Office Cyber Task Forces (FBI)
2. National Cyber Investigative Joint Task Force (FBI)
3. National Cybersecurity and Communications Integration Center (DHS)
4. US Computer Emergency Readiness Team (US-CERT) (DHS)
5. Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) (DHS)
6. Cyber Threat Intelligence Integration Center (CTIIC) (ODNI)
7. Intelligence Community Security Coordination Center (ODNI)
8. U.S. Cyber Command Joint Operations Center (NSA/DOD)
9. NSA Central Security Service Cybersecurity Threat Operations Center (NSA)
10. DOD Cyber Crime Center (DC3) (DOD)
11. State Fusion Centers
12. Networking and Information Technology Research and Development Program NITRD (PCAST/OSTP)
13. CIPAC (SCC and GCCs)

CYBER LAWS, EXECUTIVE ORDERS AND DIRECTIVES



Executive Orders and Policy Directives

PPD-21, Critical Infrastructure Security and Resilience defines 16 critical infrastructure sectors and assigns federal lead agencies (Sector-Specific Agencies) to work with them to improve critical infrastructure resilience and security using three strategies: 1) defining relationships and roles among Federal agencies, 2) ensuring efficient information exchange (including with the private sector), and 3) providing analysis of threats and incidents. DHS coordinates the SSAs and other groups in both public and private sectors. The directive also promotes long-term R&D to build the future technologies to improve security.

Executive Order 13636, Improving Critical Infrastructure Cybersecurity promotes public-private cooperation on critical infrastructure cybersecurity and outlines the process for improving critical infrastructure cybersecurity through voluntary standards and best practices. It calls on NIST to develop the Cybersecurity Framework, and DHS to publish timely unclassified reports on cyber threats and incidents in U.S. critical infrastructure.

EO 13691, Promoting Private Sector Cybersecurity Information Sharing encourages information sharing on cybersecurity threats between the private and public sectors. It calls for the creation of Information Sharing and Analysis Organizations (ISAOs), which are designed to facilitate information exchange between members or partners. DHS, through the NCCIC coordinates collaboration among ISAOs. The Order creates clear paths and processes for cyber threat and incident information but provides no exemptions from liability for companies that share data leading to legal action.

PPD-41, United States Cyber Incident Coordination seeks to clarify the Federal government's coordinated response to a significant cyber incident that could have broad effects on critical infrastructure. It also requires the National Cyber Incident Response Plan to be updated and clarify exactly whom the private sector should contact and how. The directive also addresses potential conflicts between investigating an attack, responding to return to normal operations, and drawing intelligence by stating all three proceed concurrently.

EO 13718, Commission on Enhancing National Cybersecurity is a Presidentially appointed panel of 12 experts in cybersecurity that can make specific recommendations. This Executive Order identifies specific issues for the Commission to address in a report to the President by 12/1/16. CENC was tasked to examine advanced technology for critical infrastructure that should be developed and tested, and timely approaches private sector and the government can take in light of the changing landscape of connected technologies in the US economy.

2013 2014 2015 2016

Public Laws

Federal Information Security Modernization Act (2014) and Federal Information Security Management Act (2002) ensures federal agencies that collect and maintain information on critical infrastructure implement cybersecurity practices and policies to protect that information. OMB has oversight of the policies and practices, while DHS helps to administer them.

National Cybersecurity Protection Act of 2014 establishes the National Cybersecurity and Communications Integration Center (NCCIC) at DHS to oversee critical infrastructure protection, cybersecurity, and related DHS programs. The NCCIC is intended as the federal interface with civilian entities for sharing cybersecurity risks, incidents, analysis, and warnings. It also directs DHS to make security clearances available to private sector critical infrastructure stakeholders.

Cybersecurity Enhancement Act of 2014 codifies NIST's role in the development of the Framework for Improving Critical Infrastructure Cybersecurity, (see EO 13636). The Framework and any security standards or best practices promulgated by NIST remain strictly voluntary. The Act also calls on OSTP to develop a federal cyber research and development plan.

Cybersecurity Act of 2015 addresses liability and privacy concerns of private entities when sharing information with the Federal government. The Act limits the risks of civil, regulatory, and antitrust liability when companies share threat information in accordance with this law. Although voluntary, DHS is directed to promote awareness of the information sharing programs. The NCCIC acts as the central aggregator of information on cyber threats and attacks, though DHS is not necessarily the owner of such a database.

FAST Act, Fixing America's Surface Transportation Act, Division F: Energy Security addresses cybersecurity for the electric grid. The Act codifies DOE as the Sector-Specific Agency for cybersecurity of the energy sector (see PPD-21) and gives new emergency powers to the Secretary of Energy to address cyber or physical attacks on energy infrastructure and to protect or restore services. Second, it designates certain data as "critical electric infrastructure Information," that can be readily shared with cleared industry stakeholders. Finally, it establishes an authority for private companies to recoup costs associated with complying with emergency orders from the Secretary of Energy.

What We Heard: CURRENT SITUATION

- Cyber risks to critical infrastructure are numerous and complex. Cyber protection of CI networks is often insufficient and lacks compliance mechanisms.
- Our ability to defend private sector cyber networks does not keep up with the threat. The right adversary with the right capabilities and intent can breach just about any system.
- There are serious physical consequences from a cyber attack on control systems. We can't protect everything so we need to prioritize risks and risk mitigations.
- The Federal Government has limited resources for cybersecurity leadership and expertise, and there is competition over responsibilities.
- Information sharing has improved, but still has its flaws. To be successful, information sharing needs to occur at the speed of the network.

What We Heard: CHALLENGES AND GAPS

- We still don't have frameworks in place to manage a significant disruption to infrastructure, such as a long-duration power outage.
- Greater clarity is needed on the cybersecurity roles and responsibilities of different government departments and agencies.
- Multiple Congressional committees have cyber oversight, making it difficult to get consensus on priorities for focused action.
- Smaller utilities and companies don't have the resources to identify and address unknown cyber risks.
- Much of the information and intelligence now being collected is shared, but it is not organized in a way that makes it readily usable for the private sector.
- Information sharing needs to be bi-directional but industry is reluctant to implement automated services that provide immediate response to cyber attacks.

What We Heard: FUTURE DIRECTION / ADVICE TO NIAC (1 OF 2)

- Avoid a landscape study. It will only provide a snapshot in time and is unnecessary.
- Focus on an options-based, harmonized approach to systems technology and information sharing regime as an alternative to mandatory regulations
- Examine the implications of a scaled-up, market-driven digital economy, optimized for business, that could introduce massive cyber risks that could cascade across sectors and American communities.
- The study should particularly focus on the lifeline infrastructures, such as electricity and water, and the interconnected nature of cyber.
- Focus on building cybersecurity into infrastructure and on providing assessments or guides on global supply chain risks.

What We Heard: FUTURE DIRECTION / ADVICE TO NIAC (2 OF 2)

- The study needs to look at novel approaches such as cyber resilience. Start with the assumption that your systems have been compromised.
- Look at models of innovation to understand how technology and innovation dependencies affect future cybersecurity.
- Examine the gap between current cybersecurity investments and capabilities of critical infrastructure, and the actual needs. Recommend what the government should do to close the gap.
- Examine cybersecurity risks associated with supply chains of critical infrastructure.
- Engage with key stakeholders early on to increase buy-in and the NIAC's knowledge of possible cybersecurity regulation

What We Heard: FUTURE DIRECTION / ADVICE TO NIAC (2 OF 2)

implementation issues.