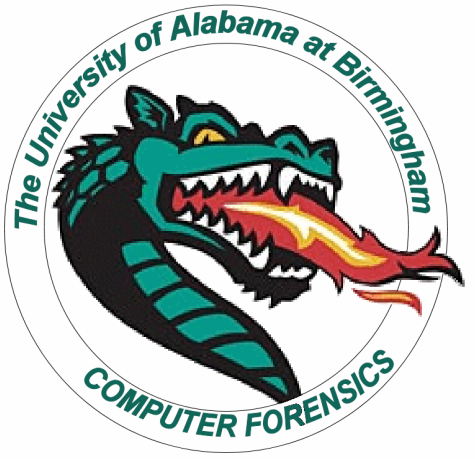

Blueprint for a Secure Cyber Future

Gary Warner

January 10, 2012

Birmingham InfraGard

DISCLAIMER

- This presentation is an attempt to SUMMARIZE the Goals and Objectives of the “Blueprint for a Secure Cyber Future”
- As such, almost all of the content is lifted from here:
- www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf
- In a few places I have abbreviated or simplified a point. The reader is advised that the original is the only true source.

The 2010 Quadrennial Homeland Security Review

Five Homeland Security Core Mission Areas

1. Prevent Terrorism and Enhance Security
2. Secure and Manage our Borders
3. Enforce and Administer our Immigration Laws
4. **Safeguard and Secure Cyberspace**
5. Ensure Resilience to Disasters

President's National Security Strategy

Declares the Nation's digital infrastructure a strategic national asset

Describes cyber threats as one of the most serious national security, public safety, and economic challenges we face as a Nation

Requires that protection of digital infrastructure be a national security priority

Cyber Threats

"Emerging cyber threats require the engagement of the entire society—from government and law enforcement to the private sector and most importantly, members of the public."

Protect Critical Information Infrastructure Today While Building a Stronger Cyber Ecosystem for Tomorrow.

VISION

Our vision is a cyberspace that supports secure and resilient infrastructure, that enables innovation and prosperity, and that protects privacy and other civil liberties by design. It is one in which we can use cyberspace with confidence to advance our economic interests and maintain national security under all conditions.

—Quadrennial Homeland Security Review Report 2010

Vision

A Cyberspace that is Secure

A Cyberspace that is Resilient

A Cyberspace that Enables Innovation

A Cyberspace that Protects Public Health and Safety

A Cyberspace that Advances Economic Interests and National Security

Guiding Principles

Privacy and Civil Liberties

Transparent Security Processes

Shared Responsibility in a Distributed Environment

Risk-based, Cost Effective, and Usable Security

Focus Area One:
Protecting Critical Information Infrastructure

Any physical or virtual information system that controls, processes, transmits, receives or stores electronic information in any form including data, voice, or video that is:

- Vital to the functioning of critical infrastructure;
- So vital to the United States that the incapacity or destruction of such systems would have a debilitating impact on national security, national economic security, or national public health and safety; or
- Owned or operated by or on behalf of a State, local, tribal, or territorial government entity.

Focus Area Two: Cyber Ecosystem

- The cyber ecosystem is global and includes government and private sector information infrastructure, the variety of interacting persons, processes, information and communication technologies, and the conditions that influence their cybersecurity.

Success: Protecting Critical Information Infrastructure

- Critical information infrastructure will be considered protected when outcome-based metrics demonstrate that owners and operators appropriately manage risks and the infrastructure is able to maintain adequate security, including confidentiality, integrity, and availability, in the face of the most consequential hazards.

Success: Strengthening the Cyber Ecosystem

- The ecosystem will be considered strong when the following conditions are met:
  - Information and communication technology risk is well defined, understood and managed by users;
  - Organizations and individuals routinely apply security and privacy standards and best practices;
  - The identities of individuals, organizations, networks, services, and devices are appropriately validated;
  - Interoperable security capabilities are built into information and communication technologies; and
  - Where appropriate, near real-time, machine-to-machine coordination provides indication, warning, and automated incident response.

Focus Area One:
Protecting Critical Information Infrastructure

GOALS

- Reduce Exposure to Cyber Risk
- Ensure Priority Response and Recovery
- Maintain Shared Situational Awareness
- Increase Resilience

Reduce Exposure to Cyber Risk

- **Avert Threats:** Decrease the ability of domestic and international criminals, including malicious insiders and foreign adversaries to exploit, impair, deny access to, or destroy critical information infrastructure
- Implement IPS
- Heighten domestic and international law enforcement activity to deter, investigate, and prosecute crimes committed through cyberspace
- Proactively identify threat actors, techniques, and procedures through all-source information collection and analysis
- Distribute timely, specific, actionable information on most dangerous threats
- Create a community of interest that engages threat information producers
- Guidelines and incentives for incident reporting

Reduce Exposure to Cyber Risk

- **Identify and Harden Critical Information Infrastructure:** Deploy appropriate security measures to manage risk to critical systems and assets.
  - Identify points most likely to affect national security, national economic security, or public health or safety – internet peering points, DNS, satellite ground stations, etc.
  - Management of networks
  - Assess and prioritize risk that a particular threat source will trigger a particular vulnerability
  - Effective risk management through implementing voluntary codes of contact
  - Continuous monitoring and measuring of internal networks
  - Standards-based automation to identify, classify and prioritize vulnerabilities and weaknesses

Reduce Exposure to Cyber Risk

- **Pursue Operational, Architectural, and Technical Innovations**: Develop new ways to address existing problems and research solutions to counter emerging security challenges.
  - R&D focused on key security priorities: Designed in Security; Tailored Trustworthy Spaces; Moving Target; and Cyber Economic Incentives
  - Rapid transition of products, tools, and capabilities from development to operation
  - Integration of national cyber R&D activities to include defense, law enforcement, counterintelligence, and homeland security research activities

Ensure Priority Response and Recovery

- **Leverage the Enterprise in Taking Priority Actions**: Unify efforts to collaboratively respond to and rapidly recover from significant cyber incidents that threaten public health or safety, undermine public confidence, have a debilitating effect on the national economy, or diminish the security posture of the Nation.
  - Timely and accurate detection, reporting, analysis, and response through watch and warning centers such as NCCCIC (National Cybersecurity and Communications Integration Center)
  - Mature and well-exercised incident response and recovery plans
  - Strong partnerships with stakeholders for rapid restoration
  - Cyber threat investigations and forensic analysis to determine the methods and paths of malicious activity, impact to infrastructure, evidence for prosecution, and inform development of countermeasures and predictive analysis. NCIJTF focal point.
  - Standards-based automated remediation capabilities

Ensure Priority Response and Recovery

- **Prepare for Contingencies:** Routinely conduct tabletop and functional exercises to test contingency plans and capture lessons learned. Core capabilities for the homeland security enterprise
  - Cross-sector exercises and simulations that assess infosharing, incident response, and incident recovery
  - Organization and sector specific processes, procedures, reporting mechanisms, information flows, and relationships
  - Continuity planning
  - Mechanism for assessing exercises and codifying lessons into policies and procedures

Maintain Shared Situational Awareness

- **Fuse Information:** Synthesize information developed through varied internal, local, national, and international sources.
  - Utilize the National Cybersecurity Protection System (NCPS) for info exchange
  - Analytic capability through people and tools to rapidly correlate information from many sources
  - Info sharing with trusted partners through fusion centers, ISACs, SCCs
  - Standardize agreements for data collection and sharing

Maintain Shared Situational Awareness

- **Distribute Information Efficiently:** Use multiple platforms to provide timely distribution of specific, actionable information.
  - Exchange timely cyber alerts through US-CERT, DOD cyber warnings, FBI InfraGard, USSS ECTF, NIST's NVD
  - System to disseminate accurate information
  - Effective communications strategies, including social media
  - Easy-to-use data portability, protecting sources and methods and originator of info
  - Economic incentives to strengthen collaboration through grants, subsidies, and tax credits

Increase Resilience

- **Increase System Fault Tolerance:** Be prepared to maintain critical operations in a degraded environment.
  - Comprehensive understanding of vulnerabilities, critical dependencides, and potential for cascading disruptions
  - Architectural guidance and standards for resilience
  - Conformance to standards for resilience such as NIST 800-34: Contingency Planning Guide for Information Technology Systems
  - Method to artificially and automatically create diversity in software systems and networks
  - Continuous audit of effectiveness of resilience strategies

phew

- That's the summary?
- What are our key points from "Protecting Critical Information Infrastructure?"

Goals for Strengthening the Cyber Ecosystem

- Empower Individuals and Organizations to Operate Securely
- Make and Use More Trustworthy Cyber Protocols, Products, Services, Configurations and Architectures
- Build Collaborative Communities
- Establish Transparent Processes

Empower individuals and Organizations to Operate Securely

- **Develop the Cyber Workforce in the Public and Private Sectors**: Maintain a strong cadre of cybersecurity professionals to design, operate, and research cyber technologies, enabling success against current and future threats.
  - Develop curriculum and encourage adoption – NICE (National Inititiave for Cybersecurity Education) has K12, plus higher ed
  - Incentives to enroll in these studies
  - Workforce retention
  - Preferred or required skills, including certification, for cybersecurity positions

Empower individuals and Organizations to Operate Securely

- **Build a Base for Distributed Security**: Provide individuals with tools, tips, education, training, awareness, and other resources appropriate to their positions that enable them to implement existing cybersecurity features and configurations in protocols, products, and services.
  - Cybersecurity awareness campaigns
  - Best practices guidelines
  - Mechanisms to notify users that their systems have weaknesses

Make and Use More Trustworthy Cyber Protocols, Products, Services, Configurations, and Architectures

- **Reduce Vulnerabilities:** Design, build, and operate information and communication technology to specifically reduce the occurrence of exploitable weaknesses. Enable technology to sense, react to, and communicate changes in its security or its surroundings in a way that preserves or enhances its security posture.
  - Leadership in standards bodies
  - Adoption of security-enabled software by users
  - Guidelines for security in system development lifecycle
  - Security product evaluation
  - Functional research to advance technology and drive standards
  - Innovation in the commercial market to address emerging threats and attack attribution
  - More agile acquisition process that specify requirements for trustworthy products and supply chain

Make and Use More Trustworthy Cyber Protocols, Products, Services, Configurations, and Architectures

- **12. Improve Usability**: Design trusted technology that is easy to use, easy to administer, rapidly customizable, and performs as expected

Build Collaborative Communities

- **13. Appropriately Validate Identities in Cyberspace:**
- **14. Increase Technical and Policy Interoperability Across Devices**
- **15. Automate Security Processes:**

Establish Transparent Processes

- **17. Publicize the Root Causes and Extent of Adverse Events in Cyberspace**
- **18. Deploy Security Measures Based on Proven Effectiveness:**
- **19. Focus on the Return on Investment**
- **20. Incentivize Performance:**

Comments Wanted

Our Chapter will be sending “feedback” based on this morning’s presentation and any additional comments we receive.

If you prefer to send your feedback directly, please feel free to respond to:

cyberfeedback@dhs.gov

We Want To Help

Gary Warner
Director of Research in Computer Forensics
A Research Partnership between
The University of Alabama at Birmingham's
Department of Computer & Information Sciences
& Department of Justice Sciences

gar@uab.edu
+1.205.422.2113

Website:
www.cis.uab.edu/forensics/

Blog:
garwarner.blogspot.com