Federal Cybersecurity Research and Development Strategic Plan

Ensuring Prosperity and National Security

Cybersecurity National Action Plan

Taking bold actions to protect Americans in today's digital world

February 2016

Cybersecurity National Action Plan

I'm confident we can unleash the full potential of American innovation, and ensure our prosperity and security online for the generations to come.

President Obama
February 9, 2016

Cybersecurity National Action Plan

Key elements:

- Establishing a **Commission on Enhancing National Cybersecurity** on improving our privacy and public safety
- Creating a **Federal Chief Information Security Officer** to lead on cybersecurity oversight, policies, and strategy
- Establishing a $3.1 billion **Information Technology Modernization Fund** to retire, replace, and modernize legacy government IT systems
- Working with industry to encourage broader use of security tools like **multi-factor authentication**

Federal Cybersecurity R&D Strategic Plan

- Requested by Congress in the *2014 Cybersecurity Enhancement Act* to update and expand the 2011 plan, *Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program*
- Written in 2015 by an interagency working group for the National Science and Technology Council (NSTC) and the Networking and Information Technology Research and Development Program (NITRD)
- Considered input from the President's Council of Advisors for Science and Technology (PCAST), an NSF RFI in May 2015, and DHS S&T community gatherings
- Released in February 2016 as a component of the President's National Cybersecurity Action Plan (CNAP)

The Need for Cybersecurity R&D

Computers and computer networking provide major benefits to modern society, yet the growing costs of malicious cyber activities and cybersecurity itself diminish these benefits.

Advances in cybersecurity are urgently needed to preserve the Internet's growing social and economic benefits by thwarting adversaries and strengthening public trust of cyber systems.

Just as brakes enable driving safely at higher speeds, cybersecurity capabilities are the foundation that accelerates innovation in cyberspace.

Cybersecurity Assumptions

- **Adversaries**. Adversaries will perform malicious cyber activities as long as they perceive that the potential results outweigh the likely effort and possible consequences for themselves
- **Defenders**. Defenders must thwart malicious cyber activities on increasingly valuable and critical systems with limited resources and despite evolving technologies and threat scenarios
- **Users**. Users—legitimate individuals and enterprises—will circumvent cybersecurity practices that they perceive as irrelevant, ineffective, inefficient, or overly burdensome
- **Technology**. As technology cross-connects the physical and cyber worlds, the risks as well as the benefits of the two worlds are interconnected

Fundamental R&D Challenge in Cybersecurity

The fundamental research challenge
is to make cybersecurity less onerous
while providing more-effective defenses

Federal Cybersecurity R&D Goals

The science, engineering, mathematics, and technology advances needed are socio-technical in nature, from foundational to applied:

- **Near-Term Goal (1-3 years).** Achieve S&T advances to counter adversaries' asymmetrical advantages with effective and efficient risk management.

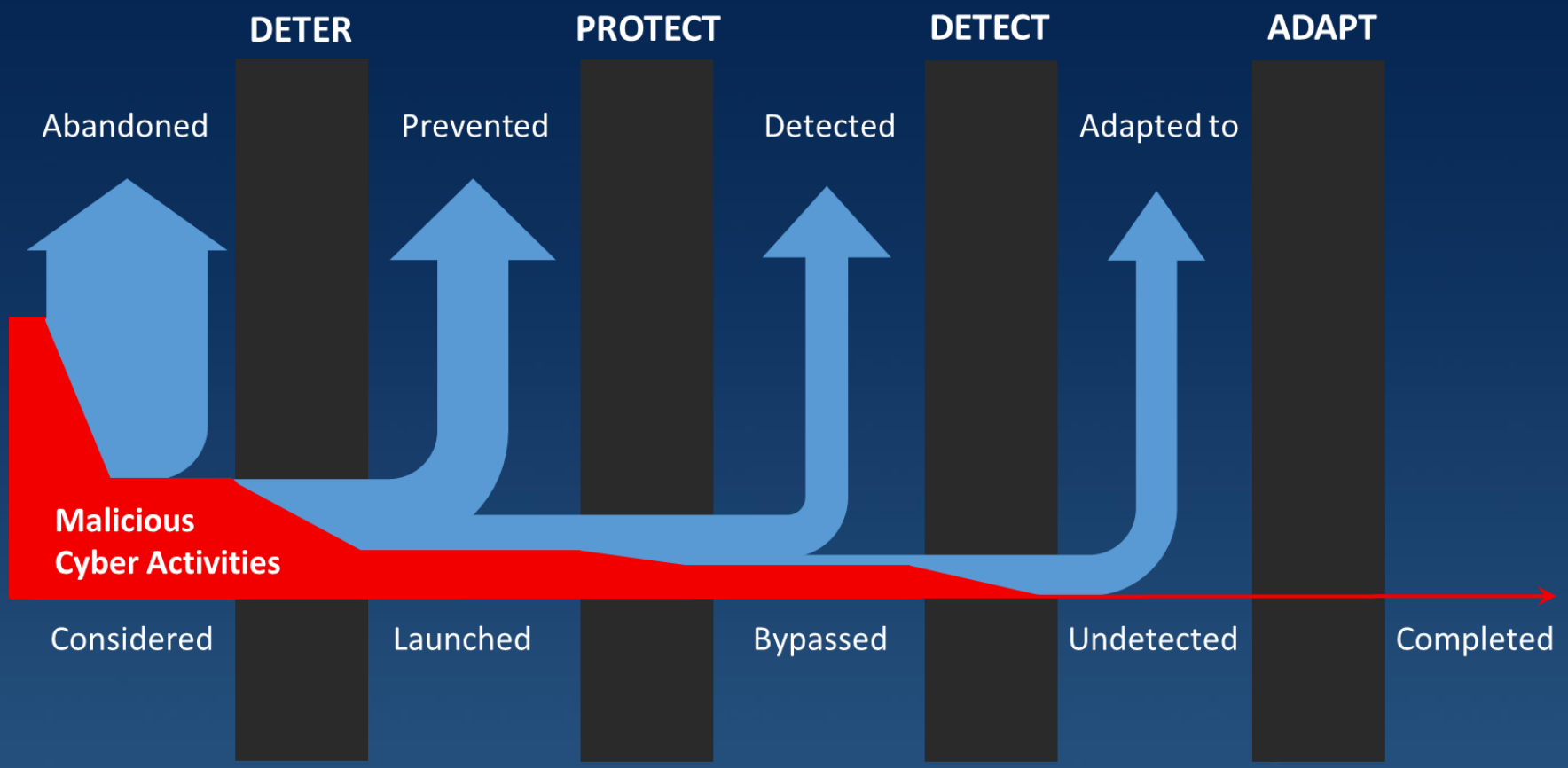
- **Mid-Term Goal (3-7 Years).** Achieve S&T advances to reverse adversaries' asymmetrical advantages, through sustainably secure systems development and operation.

- **Long-Term Goal (7-15 years).** Achieve S&T advances for effective and efficient deterrence of malicious cyber activities via denial of results and likely attribution.

Cybersecurity Defensive Elements

- **Deter.** Efficiently discourage malicious cyber activities by measuring and increasing costs to adversaries carrying out such activities, diminishing the spoils, and increasing risks and uncertainty for potential adversaries.
- **Protect.** Components, systems, users, and critical infrastructure can efficiently resist malicious cyber activities and to ensure confidentiality, integrity, availability, and accountability.
- **Detect.** Efficiently detect, and even anticipate, adversary decisions and activities, given that perfect security is not possible and systems should be assumed to be vulnerable to malicious cyber activities.
- **Adapt.** Defenders, defenses, and infrastructure can dynamically adapt to malicious cyber activities, by efficiently reacting to disruption, recovering from damage, maintaining operations while completing restoration, and adjusting to thwart similar future activity.

Federal Cybersecurity R&D Strategic Plan



Continuously strengthening defensive elements improves success in thwarting malicious cyber activities

(Figure 1. in the 2016 Federal Cybersecurity Research and Development Plan)

R&D Objectives for Defensive Elements

- Objectives highlight promising research areas and provide a basis for measuring overall progress in implementing this plan
- They do not address all areas of need and should not be considered comprehensive
- A sampling of the 21 objectives
  - Deter, near-term: Establish quantifiable metrics of adversary level of effort needed to overcome specific cybersecurity defenses
  - Protect, mid-term: Create tools for static and dynamic analysis that reduce vulnerabilities by a factor of 10
  - Detect, long-term: Develop automated tools for cyber threat forecasting
  - Adapt, long-term: Build adaptive effective collective defenses that minimize adversary-imposed effects, as well as unintended effects caused by defender actions

Critical Dependencies for Cybersecurity R&D

Success depends on advances in these areas:

- Scientific foundations
- Enhancements in risk management
- Human aspects
- Transitioning successful research into pervasive use
- Workforce development
- Enhancing the infrastructure for research

Cybersecurity for Emerging Technologies

- The defensive elements are relevant in all cybersecurity contexts. The details vary with the context.
- The Plan considers these emerging technologies and highlights specific R&D priorities for each:
  - Cyber-Physical Systems
  - Internet of Things
  - Cloud Computing
  - High Performance Computing
  - Autonomous Systems
  - Mobile Devices
- Context-based analysis needed for any technology—old or emerging

Plan Recommendations

- **Recommendation 1.** Prioritize basic and long-term research in Federal cybersecurity R&D.
- **Recommendation 2.** Lower barriers and strengthen incentives for public and private organizations that would broaden participation in cybersecurity R&D.
- **Recommendation 3.** Assess barriers and identify incentives that could accelerate the transition of evidence-validated effective and efficient cybersecurity research results into adopted technologies, especially for emerging technologies and threats.
- **Recommendation 4.** Expand the diversity of expertise in the cybersecurity research community.
- **Recommendation 5.** Expand diversity in the cybersecurity workplace.

What Does Success Look Like?

The cybersecurity research, development, and operations community will quickly design, develop, deploy, and operate effective new cybersecurity technologies and services.

Cybersecurity tasks for users will be few and easy to accomplish.

Many adversaries will be deterred from launching malicious cyber activities, and those that choose to proceed will fail or fail to impact users or organization's mission.

Information Available On-line

- Federal Cybersecurity Research and Development Strategic Plan

  https://www.whitehouse.gov/sites/whitehouse.gov/files/documents/2016_Federal_Cybersecurity_Research_and_Development_Stratgeic_Plan.pdf

- National Challenges and Goals for Cybersecurity Science and Technology

  https://www.whitehouse.gov/blog/2016/02/08/national-challenges-and-goals-cybersecurity-science-and-technology

- Cybersecurity National Action Plan

  https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan

- Commission on Enhancing National Cybersecurity

  https://www.whitehouse.gov/the-press-office/2016/02/09/executive-order-commission-enhancing-national-cybersecurity