FY2019 FEDERAL CYBERSECURITY R&D STRATEGIC PLAN IMPLEMENTATION ROADMAP

Appendix to the Networking & Information Technology Research & Development Program Supplement to the President's FY2019 Budget

Product of the
CYBER SECURITY & INFORMATION ASSURANCE
INTERAGENCY WORKING GROUP

SUBCOMMITTEE ON NETWORKING & INFORMATION
TECHNOLOGY RESEARCH & DEVELOPMENT

COMMITTEE ON SCIENCE & TECHNOLOGY ENTERPRISE

of the
NATIONAL SCIENCE & TECHNOLOGY COUNCIL

AUGUST 2018

About This Document

This document provides FY2019 implementation details for the 2016 Federal Cybersecurity Research and Development (R&D) Strategic Plan, pursuant to the Cybersecurity Enhancement Act of 2014, Public Law 113-274. It lists key Federal projects and programs that directly contribute to solving the cybersecurity challenges outlined in the 2016 Federal Cybersecurity R&D Strategic Plan. This document accompanies *the NITRD Supplement to the President's FY2019 Budget Request*, available at https://www.nitrd.gov/pubs/FY2019-NITRD-Supplement.pdf.

About the National Science and Technology Council

The NITRD Program is managed by the NITRD Subcommittee of the National Science and Technology Council (NSTC) Committee on Science and Technology Enterprise. The NSTC is the principal means by which the Executive Branch coordinates science and technology policy across the diverse entities that make up the Federal research and development enterprise. A primary objective of the NSTC is to ensure science and technology policy decisions and programs are consistent with the President's stated goals. The NSTC prepares research and development strategies that are coordinated across Federal agencies aimed at accomplishing multiple national goals. The work of the NSTC is organized under committees that oversee subcommittees and working groups focused on different aspects of science and technology. More information is available at https://www.whitehouse.gov/ostp/nstc.

About the Office of Science and Technology Policy

The Office of Science and Technology Policy (OSTP) was established by the National Science and Technology Policy, Organization, and Priorities Act of 1976 to provide the President and others within the Executive Office of the President with advice on the scientific, engineering, and technological aspects of the economy, national security, homeland security, health, foreign relations, the environment, and the technological recovery and use of resources, among other topics. OSTP leads interagency science and technology policy coordination efforts, assists the Office of Management and Budget with an annual review and analysis of Federal research and development in budgets, and serves as a source of scientific and technological analysis and judgment for the President with respect to major policies, plans, and programs of the Federal Government. More information is available at https://www.whitehouse.gov/ostp.

About the NITRD Program

The Networking and Information Technology Research and Development Program is the Nation's primary source of federally funded R&D on networking and information technology (IT). The NITRD Program seeks to maximize interagency coordination in providing the R&D foundations for continued U.S. technological leadership and meeting the needs of the Federal Government for advanced IT. The Program also seeks to accelerate development and deployment of advanced IT to support American military superiority, security, economic prosperity, energy dominance, and health, while it supports innovation and early-stage research, modernization of the IT research infrastructure, and development of a strong cyber-enabled workforce. The NITRD Program—established by the High-Performance Computing Act of 1991 (P.L. 102-194) and reauthorized by Congress in the American Innovation and Competitiveness Act of 2017 (P.L. 114-329)—is one of the oldest and largest of the formal Federal programs that engage multiple agencies in coordination activities. More information is available at https://www.nitrd.gov.

About the Cyber Security and Information Assurance Interagency Working Group

The Cyber Security and Information Assurance (CSIA) Interagency Working Group (IWG) is a Federal forum, reporting to the NITRD Subcommittee, focused on advancing solutions to many pressing cybersecurity issues through coordination of Federal cybersecurity R&D investments and activities, including developing joint research strategies and engaging academia and industry through workshops and other outreach activities. CSIA IWG agencies focus on R&D to prevent, resist, detect, respond to, and/or recover from actions that compromise or threaten to compromise the availability, integrity, or confidentiality of computer- and network-based systems. Such systems provide critical functions in every sector of the economy, as well as in national defense, homeland security, and other vital Federal missions.

Copyright Information

FY2019 FEDERAL CYBERSECURITY R&D STRATEGIC PLAN IMPLEMENTATION ROADMAP

This document provides FY2019 implementation details for the *2016 Federal Cybersecurity Research and Development Strategic Plan*,[1] developed by the Networking and Information Technology Research and Development (NITRD) Program's Cyber Security and Information Assurance (CSIA) Interagency Working Group (IWG). This Strategic Plan Implementation Roadmap is provided per statutory requirement for public provision of this information pursuant to the Cybersecurity Enhancement Act of 2014, Public Law 113-274, Section 201(a)(2)(D), Implementation Roadmap, and under direction from the NITRD Subcommittee of the National Science and Technology Council Committee on Science and Technology Enterprise. This document accompanies the *NITRD Supplement to the President's FY2019 Budget*.[2]

Agencies participating in the CSIA IWG report their research and development (R&D) programs in the Cyber Security and Privacy Program Component Area in alignment with the research objectives of the Federal Cybersecurity Research and Development Strategic Plan. The four strategic defensive elements of the strategic plan consist of Deter, Protect, Detect, and Adapt, as defined below:

- **Deter:** The ability to efficiently discourage malicious cyber activities by measuring and increasing the costs to adversaries who carry out such activities, diminishing their spoils, and increasing risks and uncertainty of consequences for cyber attacks.
- **Protect:** The ability of components, systems, users, and critical infrastructure to efficiently resist malicious cyber activities and to ensure confidentiality, integrity, availability, and accountability.
- **Detect:** The ability to 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:** The ability of defenders, defenses, and infrastructure to dynamically adapt to malicious cyber activities by efficiently reacting to disruption, recovering from damage, maintaining operations while completing restoration, and adjusting to be able to thwart similar future activity.

Listed in the roadmap table below are projects and programs being planned or carried out in fiscal years 2018, 2019, and possibly beyond, to meet the objectives of the *2016 Federal Cybersecurity Research and Development Strategic Plan*. The strategic plan provides priorities for cybersecurity R&D in alignment with the NIST *Framework for Improving Critical Infrastructure Cybersecurity*,[3] which provides guidance on managing and reducing cybersecurity risk confronted by businesses and organizations.

The programs and projects listed in Table A1 represent key agency activities in the four defensive areas, but the table is not an exhaustive listing of projects. For example, the National Science Foundation's Secure and Trustworthy Cyberspace Program is comprised of some 800 active individual grants to hundreds of researchers and their academic institutions. Likewise, programs and projects in the table vary markedly in their size and amount of funding. Programs are listed in alphabetical order by agency. Names of specific programs use title case, whereas descriptions of program types use sentence case.

[1] https://www.nitrd.gov/pubs/2016-Federal-Cybersecurity-Research-and-Development-Strategic-Plan.pdf

[2] https://www.nitrd.gov/pubs/FY2019-NITRD-Supplement.pdf

[3] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Table A1. Federal Cybersecurity R&D Strategic Plan Implementation Roadmap

FEDERAL CYBERSECURITY R&D PROGRAMS, BY AGENCY	Deter	Protect	Detect	Adapt
Air Force Research Laboratory & Air Force Office of Scientific Research				
AFOSR basic research in cybersecurity and information assurance	X	X	X	X
Agile and Resilient Embedded Systems		X	X	X
Agile Cyber Technologies		X	X	X
Assured by Design		X	X	X
Automated Cyber Survivability		X	X	X
Autonomous Defensive Cyber Operations	X	X	X	X
Autonomous Integrated Cyber Defense		X	X	X
Biologically Resilient Cyber Technology	X	X	X	X
Command and Control of Proactive Defense	X	X	X	X
Mission Awareness for Mission Assurance			X	X
Resilient and Ultra-Trusted MLS Routing		X	X	X
Army Research Laboratory and Army Communications-Electronics Research, Development, and Engineering Center				
Application Security	X	X		X
Provenance Aware Tactical Information Flows		X	X	
Reprogrammable System on Chip Universal Encryptor		X		
SDN (Software-Defined Networking) Security		X		X
Tactical Cyber Situational Understanding	X	X		
Tactical Identity and Access Management		X		
Defense Advanced Research Projects Agency				
Active Social Engineering Defense	X			
Brandeis program		X		
Building Resource Adaptive Software Systems				X
Cyber Assured Systems Engineering		X		
Cyber Fault-tolerant Attack Recovery		X		
Cyber Hunting at Scale			X	
Dispersed Computing		X		
Edge-Directed Cyber Technologies for Reliable Mission Communication				X
Enhanced Attribution	X			
Leveraging the Analog Domain for Security			X	
Plan X			X	
Rapid Attack Detection, Isolation and Characterization Systems			X	
SafeWare		X		
Space/Time Analysis for Cybersecurity		X		
System Security Integrated Through Hardware and Firmware		X		

FEDERAL CYBERSECURITY R&D PROGRAMS, BY AGENCY	**Deter**	**Protect**	**Detect**	**Adapt**
Defense Advanced Research Projects Agency (cont.)				
Transparent Computing			X	
Extreme DDoS (Distributed Denial of Service) Defense				X
Harnessing Autonomy for Countering Cyber-Adversary Systems				X
Department of Defense High-Performance Computing Modernization Program (HPCMP)				
Cybersecurity Enhancement Project		X	X	
Cybersecurity Environment for Detection, Analysis, and Reporting		X	X	
HPC Architecture for Cyber Situational Awareness		X	X	X
Information Security Continuous Monitoring—Jigsaw		X	X	
Rapid Audit of Unix		X		
Department of Homeland Security				
Botnet and malware detection and mitigation			X	
Deployable collaboration environment		X		
Malware analysis at scale	X			
Situational awareness and incident response in cloud environments	X			
Mobile		X	X	
Network Systems Security	X	X	X	X
Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response				
Cybersecurity for Energy Delivery Systems		X	X	X
National Institute of Standards and Technology				
Access control and privilege management		X		
Advanced security testing and measurement		X	X	X
Biometric standards and testing	X	X		
Cloud computing and virtualization	X	X		X
Cryptographic standards, validation, and research		X		
Identity management		X		
Information security risk management		X	X	X
Internet infrastructure protection		X	X	X
Mobile security		X		X
Privacy engineering		X		
Security of cyber-physical systems		X	X	
National Science Foundation				
Secure and Trustworthy Cyberspace Program	X	X	X	X

FEDERAL CYBERSECURITY R&D PROGRAMS, BY AGENCY	Deter	Protect	Detect	Adapt
National Security Agency				
Blended Cyber	X	X	X	X
Blended Environment		X	X	X
Cryptography in Constrained Edge Devices	X	X		
Cyber Resiliency			X	X
Eliminating Vulnerabilities	X	X		
Emerging Technologies		X	X	X
Office of Naval Research				
Cyber Attack Resilient Cyber-Physical Systems	X	X	X	
Discovery and innovation	X	X	X	X
Tools for Intrinsic Cybersecurity	X	X	X	X
Office of the Secretary of Defense				
Behavioral Cyber Sciences		X		X
Mathematical Foundations of Cyber		X		
Mission Assurance Research Collaboration			X	X
Precise Cyber Effects	X	X		
Self-Securing Systems	X	X	X	X