FY2021 FEDERAL CYBERSECURITY R&D STRATEGIC PLAN IMPLEMENTATION ROADMAP

Appendix to the Networking & Information Technology Research & Development Program Supplement to the President's FY2021 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 14, 2020

About the National Science and Technology Council

The National Science and Technology Council (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 (R&D) enterprise. A primary objective of the NSTC is to ensure that 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 Subcommittee on Networking & Information Technology Research & Development

The Networking and Information Technology Research and Development (NITRD) Program is the Nation's primary source of federally funded work on pioneering information technologies (IT) in computing, networking, and software. The NITRD Subcommittee of the NSTC Committee on Science and Technology Enterprise guides the multiagency NITRD Program in its work to provide the R&D foundations for ensuring continued U.S. technological leadership and meeting the needs of the Nation for advanced IT. The National Coordination Office supports the NITRD Subcommittee and the Interagency Working Groups (IWGs) that report to it. More information is available at https://www.nitrd.gov/about/.

About the Cyber Security and Information Assurance Interagency Working Group

The Cybersecurity 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. More information is available at https://www.nitrd.gov/groups/csia/.

About This Document

Pursuant to the Cybersecurity Enhancement Act of 2014, Public Law 113-274, this document provides FY2021 implementation details for the 2019 *Federal Cybersecurity Research and Development Strategic Plan*. It lists key Federal projects and programs that directly contribute to addressing the cybersecurity challenges outlined in the 2019 Plan. This document accompanies the *NITRD Supplement to the President's FY2021 Budget*, available at https://www.nitrd.gov/pubs/FY2021-NITRD-Supplement.pdf.

Acknowledgments

This Roadmap was developed through the contributions of NITRD's Federal agency members; representatives of other Federal agencies participating in the NITRD Program, particularly the CSIA IWG; and the NCO staff.

Published in the United States of America, 2020.

FY2021 FEDERAL CYBERSECURITY R&D STRATEGIC PLAN IMPLEMENTATION ROADMAP

This document provides FY2021 implementation plans for the 2019 *Federal Cybersecurity Research and Development Strategic Plan* (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 FY2021 Budget*.[2] In the NITRD budget supplement, agencies participating in the CSIA IWG report their research and development (R&D) programs in the Cybersecurity and Privacy Program Component Area in alignment with the research objectives of the Plan. The programs listed in the roadmap Table 1 (pp. 3–7) may address one or more of the following Defensive Elements from the Plan:

- **Deter:** The ability to efficiently discourage malicious cyber activities by increasing the costs, risks, and uncertainty to adversaries and diminishing their spoils.
- **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 systems should be assumed to be vulnerable to malicious cyber activities.
- **Respond:** The ability to dynamically react to malicious cyber activities by adapting to disruption, countering the malicious activities, recovering from damage, maintaining operations while completing restoration, and adjusting to be able to thwart similar future activities.

The programs advance the following Priority Areas defined in the Plan and contribute to implementing the Administration's vision for American leadership in the Industries of the Future (IotF):[3]

- **Artificial Intelligence (AI):** Capabilities that enable computers and other automated systems to perform tasks that have historically required human cognition and what are typically considered human decision-making abilities.
- **Quantum Information Science (QIS):** Capabilities that harness quantum mechanics and quantum material properties to achieve computation, information processing, communications, and sensing in ways that cannot be achieved with classical physics principles.
- **Trustworthy Distributed Digital Infrastructure (TDDI):** Technologies that facilitate secure information communications infrastructure that enables next-generation wireless communication, distributed computing, seamless integration of telecommunication systems with cyber-physical systems, and provides the communications infrastructure for the IotF.
- **Privacy:** Solutions that minimize privacy risks or prevent privacy violations arising from the collection and use of peoples' private information.
- **Secure Hardware and Software (HW & SW):** Technologies that provide and improve security properties of hardware and software components in computing and communication systems.

[1] https://www.nitrd.gov/pubs/Federal-Cybersecurity-RD-Strategic-Plan-2019.pdf
[2] https://www.nitrd.gov/pubs/FY2021-NITRD-Supplement.pdf
[3] https://www.whitehouse.gov/briefings-statements/america-will-dominate-industries-future/

- **Education and Workforce Development:** Programs in cybersecurity education, training, and professional development to sustain cybersecurity innovations by the national workforce.

Listed in the FY2021 roadmap Table 1 below are projects and programs that Federal agencies are planning or implementing in fiscal years 2020, 2021, and possibly beyond, to meet the objectives of the 2019 *Federal Cybersecurity Research and Development Strategic Plan*. Emphasis is given to advancing and securing the IotF, specifically as it pertains to AI, QIS, and the advanced communications networking (including fifth-generation/5G) technologies of the Trustworthy Distributed Digital Infrastructure.

The Plan provides priorities for cybersecurity R&D in alignment with the National Institute of Standards and Technology *Framework for Improving Critical Infrastructure Cybersecurity*,[4] which provides guidance on managing and reducing cybersecurity risks confronted by businesses and organizations.

The programs and projects listed in the FY2021 roadmap table represent key agency R&D activities, 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 900 active individual grants to hundreds of researchers and their academic institutions. Also, programs and projects in the table vary substantially 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 types of programs use sentence case.

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

Table 1: FY2021 Federal Cybersecurity R&D Strategic Plan Implementation Roadmap (p. 1 of 5)

FEDERAL CYBERSECURITY R&D PROGRAMS, BY AGENCY	DEFENSIVE ELEMENTS				PRIORITY AREAS					
	Deter	Protect	Detect	Respond	AI	QIS	TDDI	Privacy	Secure HW & SW	Education/ Workforce
Air Force Office of Scientific Research (AFOSR) and Air Force Research Laboratory (AFRL)										
AFOSR: Assured autonomy in contested environments	X	X	X	X	X			X		X
AFOSR: Center for Enabling Cyber Defense in Analog and Mixed Signal Domain		X	X	X					X	X
AFOSR: Language-based security		X	X		X			X		
AFOSR: Nanoscale security		X	X			X		X	X	
AFOSR: Physical resources for security		X	X			X		X		
AFOSR: Security of nonlinear hybrid systems	X	X	X	X						
AFRL: Advanced Course in Engineering										X
AFRL: Agile Means of Power Projection			X	X						
AFRL: Automated Cyber Survivability		X	X	X						
AFRL: Computational Diversity for Cyber Security	X	X							X	
AFRL: Enhanced T-CORE Platform	X	X							X	
AFRL: Highly Assured and Defended Embedded Systems		X	X	X						
AFRL: Nova: System vulnerability assessment		X								
Army Futures Command/Combat Capabilities Development Command: Army Research Laboratory (ARL) and Army Research Office (ARO); and Command, Control, Computers, Communications, Cyber, Intelligence, Surveillance, and Reconnaissance Center (C5ISR)										
ARL: Agile Cyber Maneuver & Resilience	X		X		X					
ARL: Autonomous Active Cyber Defense			X	X	X					
ARL: Camouflage and Decoy of CEMA (cyber and electromagnetic activities) for Network Survivability	X			X	X					

Table 1: FY2021 Federal Cybersecurity R&D Strategic Plan Implementation Roadmap (p. 2 of 5)

FEDERAL CYBERSECURITY R&D PROGRAMS, BY AGENCY	DEFENSIVE ELEMENTS				PRIORITY AREAS					
	Deter	Protect	Detect	Respond	AI	QIS	TDDI	Privacy	Secure HW & SW	Education/ Workforce
ARL, ARO, and C5ISR (*cont.*)										
ARL & C5ISR: Cyber Research Alliance / Applied Research Evaluation Partner	X		X	X	X		X			
ARO: Cyber Adaption Multidisciplinary University Research Initiative			X	X	X					
ARO: Cyber Deception Multidisciplinary University Research Initiative	X									
C5ISR: Agile Virtual Enclave		X								
C5ISR: Autonomous Cyber		X	X	X	X					
C5ISR: Information Trust		X	X	X	X		X			
C5ISR: Network Obfuscation/Deception	X			X	X					
Defense Advanced Research Projects Agency										
Active Social Engineering Defense	X									
Assured Micropatching		X								
Computers and Humans Exploring Software Security	X									
Configuration Security		X								
Cyber Assured Systems Engineering		X								
Cyber-Hunting at Scale			X							
Dispersed Computing		X								
Enhanced Attribution	X									
Harnessing Autonomy for Countering Cyber-Adversary Systems				X						
Intent Defined Adaptive Software		X								
Open, Programmable, Secure 5G		X								
Resilient Anonymous Communication for Everyone		X								
Securing Information for Encrypted Verification & Evaluation		X								

Table 1: FY2021 Federal Cybersecurity R&D Strategic Plan Implementation Roadmap (p. 3 of 5)

FEDERAL CYBERSECURITY R&D PROGRAMS, BY AGENCY	DEFENSIVE ELEMENTS				PRIORITY AREAS					
	Deter	Protect	Detect	Respond	AI	QIS	TDDI	Privacy	Secure HW & SW	Education/ Workforce
Department of Defense (DOD) High-Performance Computing Modernization Program										
Cybersecurity Analysis for Critical Infrastructure Resilience		X	X		X					
Cybersecurity Environment for Detection, Analysis, and Reporting		X	X		X					
HPC Architecture for Cyber Situational Awareness		X	X		X					
Rapid Audit of Unix		X								
DOD Office of the Secretary of Defense										
Applied Mathematics: Mitigating Adversarial Machine Learning	X		X	X	X				X	
Applied Mathematics: Stealthy Communications and Situational Awareness		X	X						X	
Behavioral Cyber Science: Designing Contextualized Operator Perspective to Enable Joint Cyber Operations		X								X
Behavioral Cyber Science: Performance Assessment Suite for the Cyber Mission Force		X								X
Precise Cyber Effects: Autonomous Recognition and New Generation of Exfiltration Links		X	X							
Precise Cyber Effects: Precision Cyber Effect Discovery and Assessment	X	X	X		X					
Precise Cyber Effects: Secure Coexistence of Advanced Wireless Networks		X	X				X			
Self-Securing Systems: Autonomous Cyber Defense	X	X	X	X						
Self-Securing Systems: Autonomous Intelligent Resilient Security		X	X	X	X					
Self-Securing Systems: Robust Low-Level Cyber Attack Resilience for Warfighting Vehicles		X	X	X	X					

Table 1: FY2021 Federal Cybersecurity R&D Strategic Plan Implementation Roadmap (p. 4 of 5)

FEDERAL CYBERSECURITY R&D PROGRAMS, BY AGENCY	DEFENSIVE ELEMENTS				PRIORITY AREAS					
	Deter	Protect	Detect	Respond	AI	QIS	TDDI	Privacy	Secure HW & SW	Education/ Workforce
Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response										
Cybersecurity for Energy Delivery Systems		X	X	X	X	X	X		X	X
Department of Homeland Security										
Cyber Data Analytics		X								
Industrial Control Systems and Cyber Physical Security		X					X			
Mobile Device and Application Security		X	X						X	
National Institute of Standards and Technology										
Advanced research and application development	X	X	X		X		X		X	
Awareness and workforce										X
Cryptography	X	X				X				
Identity	X	X	X	X						
Internet infrastructure		X	X				X			
Risk management		X	X	X	X			X		
Securing emerging technologies					X	X	X	X	X	
Testing and measurement		X	X						X	
National Science Foundation										
Secure and Trustworthy Cyberspace Program	X	X	X	X	X	X	X	X	X	X
National Security Agency										
Autonomous Cyber Defense				X	X					
Boutique analyses	X								X	
Centaur-style analyses	X								X	
Camo			X							
Data Fusion			X							

Table 1: FY2021 Federal Cybersecurity R&D Strategic Plan Implementation Roadmap (p. 5 of 5)

FEDERAL CYBERSECURITY R&D PROGRAMS, BY AGENCY	DEFENSIVE ELEMENTS				PRIORITY AREAS					
	Deter	Protect	Detect	Respond	AI	QIS	TDDI	Privacy	Secure HW & SW	Education/ Workforce
National Security Agency (*cont.*)										
IoT (Internet of Things) Trust Anchors		X							X	
Mitigating Adversarial Machine Learning			X		X					
ONRAMP II										X
Science of Security		X	X				X	X		
Secure Wearable Authentication Gear		X							X	
Security Enhancements–Internet of Things		X							X	
Office of Naval Research										
Crypto Factory		X						X	X	
Cyber Moat	X	X			X					
HERCULE: Harmful Episode Reconstruction by Correlating Unsuspicious Logged Events	X		X		X					
MalSee			X		X					
Noise Factory	X			X	X					
Popcorn Linux	X									
Resilient Hull, Mechanical, and Electrical Security	X	X	X	X	X		X		X	
Reverse Formal		X	X						X	
Total Platform Cyber Protection	X	X	X	X	X		X		X	