FY2022 Federal Cybersecurity R&D Strategic Plan Implementation Roadmap

Appendix to the Networking & Information Technology Research & Development Program and the National Artificial Intelligence Initiative Office Supplement to the President's FY2022 Budget

A report by the

CYBER SECURITY & INFORMATION ASSURANCE
INTERAGENCY WORKING GROUP

SUBCOMMITTEE ON NETWORKING AND INFORMATION TECHNOLOGY
RESEARCH AND DEVELOPMENT

COMMITTEE ON SCIENCE AND TECHNOLOGY ENTERPRISE

of the

NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

December 2021

About the National Science and Technology Council

Established by Executive Order on November 23, 1993, the National Science and Technology Council (NSTC) coordinates science and technology (S&T) policy across the Federal research and development (R&D) agencies. Chaired by the President, the membership of the Cabinet-level National Science and Technology Council includes the Vice President, Director of the Office of Science and Technology Policy, and Cabinet Secretaries and Agency Heads with significant S&T responsibilities. A primary objective of the NSTC is to establish clear national goals for Federal S&T investments in a broad array of areas spanning virtually all the mission areas of the Executive Branch. The NSTC prepares R&D strategies that are coordinated across agencies to ensure that the Federal Government's investment packages and policies are smart and aimed at accomplishing multiple national goals. (https://www.whitehouse.gov/ostp/nstc/)

About the Office of Science and Technology Policy

Congress established the White House Office of Science and Technology Policy (OSTP) in 1976 to advise the President and others within the Executive Office of the President on scientific, engineering, and technological aspects of the economy, national security, homeland security, health, foreign relations, and the environment. OSTP leads efforts across the Federal Government to develop and implement sound science and technology policies, plans, programs, and budgets, and it works with the private and philanthropic sectors; state, local, tribal, and territorial governments; the research and academic communities; and other nations toward this end. OSTP also assists the Office of Management and Budget with its annual review and analysis of Federal R&D in budgets. OSTP's Senate-confirmed Director co-chairs the President's Council of Advisors on Science and Technology and the NSTC. (https://www.whitehouse.gov/ostp/nstc/)

About the Subcommittee on Networking & Information Technology Research & Development

The Networking and Information Technology Research and Development (NITRD) Program has been the Nation's primary source of federally funded work on pioneering information technologies (IT) in computing, networking, and software since it was first established as the High Performance Computing and Communications program following passage of the High Performance Computing Act of 1991. 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 Nation's needs for advanced IT. The National Coordination Office (NCO) supports the NITRD Subcommittee and its Interagency Working Groups (IWGs). (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. 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. (https://www.nitrd.gov/groups/csia/)

About This Document

Pursuant to the Cybersecurity Enhancement Act of 2014, Public Law 113-274, this document provides FY2022 implementation details for the 2019 *Federal Cybersecurity Research and Development Strategic Plan*. It lists key Federal R&D programs that directly contribute to addressing the cybersecurity challenges outlined in the 2019 Plan. This document accompanies the *NITRD-NAIIO Supplement to the President's FY2022 Budget Request* (NAIIO is the National AI Initiative Office) available at https://www.nitrd.gov/pubs/FY2022-NITRD-NAIIO-Supplement.pdf.

Copyright Information

FY2022 FEDERAL CYBERSECURITY R&D STRATEGIC PLAN IMPLEMENTATION ROADMAP

This document provides FY2022 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 Program and the National Artificial Intelligence Initiative Office Supplement to the President's FY2022 Budget*.[2] In the 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 also advance one or more of the following Priority Areas defined in the Plan:

- **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 Industries of the Future (IotF).

[1] https://www.nitrd.gov/pubs/Federal-Cybersecurity-RD-Strategic-Plan-2019.pdf

[2] The National Artificial Intelligence Initiative Office reports in the FY2022 Supplement for the first time on the National Artificial Intelligence Research and Development Institutes mandated by the National Artificial Intelligence Initiative of 2020. https://www.nitrd.gov/pubs/FY2022-NITRD-NAIIO-Supplement.pdf

- **Privacy:** Solutions that minimize privacy risks or prevent privacy violations arising from the collection and use of people's 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.
- **Education and Workforce Development:** Programs in cybersecurity education, training, and professional development to sustain cybersecurity innovations by the national workforce.

Listed in the FY2022 roadmap Table 1 below are programs that Federal agencies are planning or implementing in fiscal years 2021, 2022, and possibly beyond, to meet the objectives of the 2019 Federal Cybersecurity Research and Development Strategic Plan. Emphasis is given to advancing and securing AI, QIS, and the 5G/advanced communications 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*,[3] which provides guidance on managing and reducing cybersecurity risks confronted by businesses and organizations.

The programs listed in the FY2022 roadmap table represent key agency R&D activities, but the table is not an exhaustive listing of current or planned activities. For example, the National Science Foundation's Secure and Trustworthy Cyberspace Program is comprised of some 1,000 active individual grants to hundreds of researchers and their academic institutions. Also, programs 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.

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

Table 1: FY2022 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)										
Advanced Course in Engineering										X
Agile Means of Power Projection	X									
Computational Diversity for Cyber Security		X								
Cybersecurity Basic Research	X	X	X	X	X	X				
Information Assurance Fellowship										X
ISR Trusted Toolkit for Attritables: Secure Trusted Environment									X	
Nova: System vulnerability assessment		X								
Secure Extreme Embedded Exploitation/Processing Onboard									X	
Secure Mobile Digital Ops							X			
Secure and Resilient Computing on Untrusted Multi-clouds							X			
Virtual Institutes for Cyber and Electromagnetic Spectrum Research and Employ										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: Camouflage and Decoy of CEMA (cyber and electromagnetic activities) for Network Survivability	X			X	X					
ARL: Tactical Autonomous Active Cyber Defense			X	X	X					
ARL & C5ISR: Cyber Research Alliance / Applied Research Evaluation Partner	X		X	X	X		X			
ARO: Autonomous Active Cyber Defense Multidisciplinary University Research Initiative				X	X					

Table 1: FY2022 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.)										
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			
Defense Advanced Research Projects Agency (DARPA)										
Active Social Engineering Defense	X				X					
Assured Micropatching		X							X	
Computers and Humans Exploring Software Security	X				X				X	
Configuration Security		X			X				X	
Cyber Assured Systems Engineering		X			X				X	
Cyber-Hunting at Scale			X		X					
Dispersed Computing		X					X			
Enhanced Attribution	X				X					
Harnessing Autonomy for Countering Cyber-Adversary Systems				X	X					
Intent Defined Adaptive Software		X			X				X	
Open, Programmable, Secure 5G		X					X		X	
Resilient Anonymous Communication for Everyone		X					X			
Securing Information for Encrypted Verification & Evaluation		X					X			
Verified Security and Performance Enhancement of Large Legacy Software		X							X	

Table 1: FY2022 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 Enhancement Project		X	X	X						
Cybersecurity Environment for Detection, Analysis, and Reporting		X	X		X					
HPC Architecture for Cyber situational Awareness		X	X		X					
Operationalizing the Cybersecurity Framework		X	X		X					
DOD Office of the Secretary of Defense										
AI-Augmented Capabilities/Cyber Defense/Enabled Tools	X	X	X	X	X					
Countering Adversary Influence	X		X	X	X				X	X
Delivering Continuous Reasoning with DevSecOps		X	X		X				X	
NDAA FY2019 Section 1640 (VICEROY): Cyber Institutes at Institutions of Higher Learning		X								X
NDAA FY2020 Section 257: 25-Year Roadmap for S&T Activities to Support Cyber	X	X	X	X	X					
Precision Cyber Effects Discovery and Assessment		X	X	X	X		X			
Quantitative Measurement of Cyber Resilience of Military Systems		X	X	X	X					
Transition of Joint DoD and Commercial Vehicle Cyber Security Efforts	X	X	X	X	X					
Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response										
Cybersecurity for Energy Delivery Systems		X	X	X	X	X	X		X	X

Table 1: FY2022 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 Homeland Security										
Cyber Analytics and Platform Capabilities	X	X	X	X	X			X	X	
Cyber Innovation Lab		X	X	X	X			X		X
Cyber Quality Assurance and Resilient Operations	X	X							X	
Secure and Resilient Mobile Network Infrastructure	X	X	X	X					X	
Software Assurance Landscape Analysis		X	X						X	
Software Supply Chain Identification SBIR			X		X				X	
National Institute of Standards and Technology										
Cryptography	X	X								
Emerging technologies		X								
Identity and access management	X	X								
National Initiative for Cybersecurity Education										X
Post-quantum cryptography						X				
Privacy program								X		
Risk management	X	X	X	X						
Trustworthy AI					X					
Trustworthy networks								X		
Trustworthy platforms									X	
National Institutes of Health										
Civic Digital Fellowship										X
Clinical data intelligence and advanced analytics					X					
Secure and privacy-preserving genome-wide and phenome-wide association studies via Intel Software Guard Extensions								X		
Secure and Private Collaborative Environments									X	

Table 1: FY2022 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 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-styled analyses	X								X	
Camo			X							
Data Fusion			X							
Interrogating neural networks with formal methods					X					
IoT Trust Anchors		X							X	
K-12 bootstrapping activities										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	
Verification of fairness of machine learning models					X					
Office of Naval Research										
Cyber deception	X			X	X				X	
Foundations of high-assurance systems		X	X						X	
Physics-aware and adversary-tolerant systems		X							X	
Real-time planning				X	X				X	
Total Platform Cyber Protection		X	X	X	X				X	X
U.S. Naval Academy research projects										X