FY 2023 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 FY 2023 Budget

A report by the

CYBER SECURITY & INFORMATION ASSURANCE
INTERAGENCY WORKING GROUP

SUBCOMMITTEE ON NETWORKING AND INFORMATION TECHNOLOGY
RESEARCH AND DEVELOPMENT

of the

NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

November 2022

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, health, foreign relations, and the environment, 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 R&D 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 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 science and technology policy decisions and programs are consistent with the President's stated goals. The NSTC prepares R&D 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 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 guides the multiagency NITRD Program in its work to provide the R&D foundations for ensuring continued U.S. technological leadership and for 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) coordinates Federal cybersecurity R&D and supports research activities to protect U.S. information, information systems, and people from cyber threats. This R&D supports the security and safety of U.S. information systems that sustain the capabilities and technologies, including power generation, transportation, finance, healthcare, manufacturing, and national security missions, within many sectors (https://www.nitrd.gov/groups/csia/).

About This Document

Pursuant to the Cybersecurity Enhancement Act of 2014, Public Law 113-274, this document provides FY 2023 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 FY 2023 Budget Request* (NAIIO is the National AI Initiative Office) available at https://www.nitrd.gov/pubs/FY2023-NITRD-NAIIO-Supplement.pdf.

Copyright Information

FY 2023 Federal Cybersecurity R&D Strategic Plan Implementation Roadmap

This document provides FY 2023 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 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.

This document accompanies the *NITRD Program and the National Artificial Intelligence Initiative Office Supplement to the President's FY 2023 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 this Roadmap 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 and risks, increasing uncertainty for 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, under the assumption that all systems are 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 deterring future threats.

The programs may 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, and seamless integration of telecommunication systems with cyber-physical systems, and that provide the communications infrastructure for the Industries of the Future.

[1] https://www.nitrd.gov/pubs/FY2022-Cybersecurity-RD-Roadmap.pdf
[2] https://www.nitrd.gov/publications/

- **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 and SW)**: Technologies that provide and improve security properties of HW and SW 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 Table 1 (pages 3–7) of the Roadmap are programs that Federal agencies are planning or implementing in fiscal years 2022, 2023, 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 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 composed 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: FY 2023 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
Critical Infrastructure Resiliency and Prediction of Cascading Effects		X								
Cyber BlackBox									X	
Cybersecurity Basic Research	X	X	X	X	X	X			X	X
Fundamentals of Cyber Science		X								
Information Assurance Fellowship										X
Resilient and Secure Computing on Untrusted Clouds							X			
SALIENT GHOST							X			
Secure Extreme Embedded Exploitation and Processing Onboard									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: Quantum Information Science						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: AI/ML for Spectrum situational awareness					X					
ARO: Autonomous Active Cyber Defense Multidisciplinary University Research Initiative				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								

Table 1: FY 2023 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.)										
C5ISR: Autonomous Cyber		X	X	X	X					
C5ISR: Information Trust		X	X	X	X					
C5ISR: Public Key Infrastructure (PKI) Modernization & Dynamic Access Control		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					
Hardening Development Toolchains Against Emergent Execution		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: FY 2023 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)										
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/ML for IoT Wireless Protocol Monitoring and Anomaly Detection			X		X					
Countering Adversary Influence	X		X	X	X					
Cyber Agreements for Resilience Machines Through Augmented AI	X	X	X	X	X					
Delivering Continuous Reasoning with DevSecOps		X			X				X	
NDAA FY 2019 Section 1640 (VICEROY): Cyber Institutes at Institutions of Higher Learning										X
Precision Cyber Effects Discovery and Assessment		X		X	X					
Quantitative Measurement of Cyber Resilience of Military Systems		X		X						
Rainfly		X		X						
SALIENT GHOST		X					X		X	
Transition of Joint DoD and Commercial Vehicle Cyber Security Efforts		X	X	X						
Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response										
Risk Management Tools & Technologies		X	X	X	X	X	X		X	X

Table 1: FY 2023 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 Platform Capabilities			X	X	X					
CISA Advanced Analytics Platform for Machine Learning	X	X			X					
Joint Analytic Collaboration Environment	X	X			X					
Mobile Threat Hunting			X	X	X					
Software Assurance									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					
NIH Research Authentication Service		X					X			
Privacy-preserving genomic medicine analysis								X		
Secure and privacy-preserving genome-wide and phenome-wide association studies		X							X	

Table 1: FY 2023 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										
Cybersecurity Innovation for Cyberinfrastructure	X	X	X	X	X			X	X	X
Secure and Trustworthy Cyberspace Program	X	X	X	X	X	X	X	X	X	X
National Security Agency										
5G Cybersecurity		X					X			
Autonomous Cyber Defense	X			X	X					
Boutique analyses	X									
Camo			X							
Centaur-styled analyses	X			X						
Cyber Threat Intelligence			X							
Data Fusion			X		X					
OnRamp II										X
Science of Security		X								X
Secure supply chain		X							X	
Security enhancements–Linux		X							X	
Office of Naval Research										
Legacy systems		X							X	
Ship-board resilience				X					X	
Supply chain security			X						X	
Total Platform Cyber Protection		X	X	X	X				X	X
U.S. Naval Academy, STEM										X