FY 2024 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 2024 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 2023

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 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

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)

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/coordination-areas/csia/)

About This Document

Pursuant to the Cybersecurity Enhancement Act of 2014, Public Law 113-274, this document provides FY 2024 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 2024 Budget Request* (NAIIO is the National AI Initiative Office) available at https://www.nitrd.gov/pubs/FY2024-NITRD-NAIIO-Supplement.pdf.

Copyright Information

FY 2024 Federal Cybersecurity R&D Strategic Plan Implementation Roadmap

This document provides FY 2024 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),[2] 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 2024 Budget*.[3] 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 Table 1 (pp. 3–8) 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 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, seamless integration of telecommunication systems with cyber-physical systems, and provides the communications infrastructure for the Industries of the Future.
- **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.

[1] https://www.nitrd.gov/pubs/Federal-Cybersecurity-RD-Strategic-Plan-2019.pdf. As directed by the Cybersecurity Enhancement Act of 2014, a quadrennial update of the Federal Cybersecurity R&D Strategic Plan will be released by the National Science and Technology Council by December 31, 2023.

[2] https://www.govinfo.gov/content/pkg/PLAW-113publ274/pdf/PLAW-113publ274.pdf

[3] https://www.nitrd.gov/pubs/FY2024-NITRD-NAIIO-Supplement.pdf

Listed in Table 1 below are programs that Federal agencies are planning or implementing in fiscal years 2023, 2024, 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*,[4] which provides guidance on managing and reducing cybersecurity risks confronted by businesses and organizations.

The programs listed in Table 1 below 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.

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

Table 1: FY 2024 Federal Cybersecurity R&D Strategic Plan Implementation Roadmap (p. 1 of 6)

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
Automated Vulnerability Identification Prioritization for Embedded Resources									X	
Circat Breaker		X								
Cybersecurity Basic Research	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 On-board									X	
ToolS to Quantify & Assure Agile SW Dev Cycle									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 (C5ISR) Center										
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: Cyber Collaborative 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					
ARL: Talent Management										X

Table 1: FY 2024 Federal Cybersecurity R&D Strategic Plan Implementation Roadmap (p. 2 of 6)

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 C5IR (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					
C5ISR: Network Obscuration	X	X	X	X	X					
C5ISR: Public Key Infrastructure Modernization & Dynamic Access Control		X								
C5ISR: Tactical Hardening for Quantum		X				X				
C5ISR: Tactical Zero Trust	X	X								
Defense Advanced Research Projects Agency										
Assured Micropatching		X							X	
Carcosa			X		X					
Constellation		X			X					
Hardening Development Toolchains Against Emergent Execution		X							X	
Open, Programmable, Secure 5G		X					X		X	
Resilient Anonymous Communication for Everyone		X					X			
Securing Information for Encrypted Verification & Evaluation		X					X			
Signature Management using Operational Knowledge and Environments	X				X					
Verified Security and Performance Enhancement of Large Legacy Software		X							X	

Table 1: FY 2024 Federal Cybersecurity R&D Strategic Plan Implementation Roadmap (p. 3 of 6)

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										
Augmented Cyber Cognition with Operational Learning Automation of Deployable Expertise			X	X	X					
Cyber Agreements for Resilience Machines through Augmented AI	X	X	X	X	X					
NDAA FY 2019 Section 1640 (VICEROY): Cyber Institutes at Institutions of Higher Learning										X
University Consortium for Cybersecurity										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
Department of Homeland Security (DHS)										
Critical Infrastructure Security & Resilience Research	X	X					X		X	
Cyber Analytics Platform Capabilities			X	X	X					
Cyber Analytics Platform – Machine Learning	X	X	X	X	X					
Cybersecurity for Law Enforcement		X								X
Cybersecurity Threats Technology Center	X	X	X	X	X			X		
Data Analytics Technology Center		X	X	X	X			X		
Mobile Threat Hunting			X	X	X					
Natural Language Processing		X	X	X	X					

Table 1: FY 2024 Federal Cybersecurity R&D Strategic Plan Implementation Roadmap (p. 4 of 6)

FEDERAL CYBERSECURITY R&D PROGRAMS, By AGENCY	Defensive Elements				Priority Areas					
	Deter	Protect	Detect	Respond	AI	QIS	TDDI	Privacy	Secure HW & SW	Education/ Workforce
DHS (cont.)										
Maritime Cyber Security Testbed	X	X	X							
Quantum Information Science Research Activity						X				
Software Assurance, Maturity, and Composition			X	X	X				X	
National Institute of Standards and Technology										
Cryptography	X									
Emerging technologies R&D				X						
Identity and access management		X								
IT forensics			X							
National Initiative for Cybersecurity Education										X
National Vulnerability Database			X							
Privacy Engineering/Privacy-Enhancing Cryptography								X		
Quantum Information Science						X				
Risk management		X								
Trustworthy AI					X					
Trustworthy Digital Infrastructure							X			
Trustworthy hardware	X								X	
Trustworthy software	X								X	
National Institutes of Health (NIH)										
AuthM: Authorization Distribution		X	X	X			X		X	
AuthM: Connectivity Management	X	X					X			
AuthM: ZTA Message Protocols		X	X				X		X	
Collaboration with NIST/NCCoE		X						X		

Table 1: FY 2024 Federal Cybersecurity R&D Strategic Plan Implementation Roadmap (p. 5 of 6)

Federal Cybersecurity R&D Programs, by Agency	Defensive Elements				Priority Areas					
	Deter	Protect	Detect	Respond	AI	QIS	TDDI	Privacy	Secure HW & SW	Education/ Workforce
NIH (cont.)										
Covid-19 Tracing			X							
De-Identification								X		
NIH and DOE Collaboration					X	X		X		
NIH Cloud Platform Interoperability							X			
Science and Technology Research Infrastructure for Discovery, Experimentation, and Sustainability							X			
Privacy-preserving encryption								X		
Trusted Execution Environments								X	X	
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										
Autonomous Cyber Defense	X			X	X					
Camo			X							
Data Fusion/Graphs			X		X					
Human Machine Teaming for Software Analysis	X			X						
OnRamp II										X
Science of Security		X								X
Secure supply chain		X							X	
Security Enhancements–Linux Policy		X							X	
Security Systems Architecture/Analyses	X									
5G and NextG cybersecurity		X					X			

Table 1: FY 2024 Federal Cybersecurity R&D Strategic Plan Implementation Roadmap (p. 6 of 6)

Federal Cybersecurity R&D Programs, by Agency	Defensive Elements				Priority Areas					
	Deter	Protect	Detect	Respond	AI	QIS	TDDI	Privacy	Secure HW & SW	Education/ Workforce
Office of Naval Research										
Autonomy		X	X	X	X				X	
Cyber-Warriors		X								X
Deception	X			X					X	
Secure and Reliant Cyber Physical Systems		X		X					X	
Supply chain security			X						X	
U.S. Naval Academy, STEM										X
Department of Agriculture										
AI Innovation, Digital Agriculture, Data Infrastructure	X	X	X	X	X			X	X	X
IT forensics for Ag biological threats	X	X	X	X	X					
Trustworthy AI					X					
Trustworthy Digital Infrastructure							X			
Trustworthy Hardware	X								X	
Trustworthy Software	X								X	