Appendix A: FY2025 Cybersecurity R&D Strategic Plan
Implementation Roadmap

The Networking & Information Technology Research & Development Program and the
National Artificial Intelligence Initiative Office Supplement to the President's FY2025 Budget

FY2025 FEDERAL CYBERSECURITY R&D STRATEGIC PLAN IMPLEMENTATION ROADMAP

A report by the

CYBERSECURITY & INFORMATION ASSURANCE
INTERAGENCY WORKING GROUP

SUBCOMMITTEE ON NETWORKING AND INFORMATION TECHNOLOGY
RESEARCH AND DEVELOPMENT

of the

NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

November 2024

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 Cybersecurity 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 FY2025 implementation details for the 2023 *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 2023 Plan. This document accompanies the *NITRD-NAIIO Supplement to the President's FY2025 Budget Request* (NAIIO is the National AI Initiative Office) available at https://www.nitrd.gov/pubs/FY2025-NITRD-NAIIO-Supplement.pdf.

Copyright Information

Disclaimer

Any mention in the text of commercial, non-profit, academic partners, or their products, or references is for information only; it does not imply endorsement or recommendation by any U.S. government agency.

FY2025 FEDERAL CYBERSECURITY R&D
STRATEGIC PLAN IMPLEMENTATION ROADMAP

This document provides FY2025 implementation plans for the 2023 *Federal Cybersecurity Research and Development Strategic Plan* (Plan),[1] developed by the Networking and Information Technology Research and Development (NITRD) Program's Cybersecurity 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 FY2025 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 priorities of the Plan. The programs listed in Table 1 may address one or more of the following research priorities from the Plan:

Cybersecurity Through Human-centered Approaches: Develop capabilities to effectively incorporate human and societal values, needs, and abilities into the design, development, operation, and evaluation of information systems and cybersecurity solutions.

Empower Organizations to Tackle Cybersecurity Threats: Develop methods, techniques to understand, analyze, and manage cyber security, cyber resilience, and privacy risks. Advance methods, techniques to understand how markets, liabilities, incentives, insurance, and regulation could ensure better cyber security and cyber resilience outcomes.

Cybersecurity Education and Workforce Development: Programs in cybersecurity education, training, professional development, and public awareness. Develop capabilities to improve the productivity of the cybersecurity workforce.

Establish and Negotiate Trust: Develop capabilities to establish, enforce, and verify the desired level of trust at all layers of computing (e.g., hardware, operating systems, applications, networking, information exchanges). Develop capabilities to establish and ensure trust for identity, access, and interoperation.

Cyber Resilience by Design: Develop methods and approaches for designing, developing, and validating systems that can withstand and recover from cyberattacks and continue to deliver vital functions even when compromised. Advance science and engineering of cyber resilience.

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 Federal Priority Application Scenarios defined in the Plan:

[1] https://www.nitrd.gov/pubs/Federal-Cybersecurity-RD-Strategic-Plan-2023.pdf

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

[3] https://www.nitrd.gov/pubs/FY2025-NITRD-NAIIO-Supplement.pdf

Protect Software (SW) and Hardware (HW) Supply Chain: Advance capabilities to attest to SW and HW supply chain integrity through design and development, and to verify and maintain ongoing supply chain integrity throughout operations.

Realize Secure and Trustworthy Artificial Intelligence (AI): Develop capabilities to realize AI that is verifiably safe, secure, and resilient. Develop capabilities that improve trusted collaboration between humans and AI.

Secure Clean Energy Future: Develop methods, technologies, and capabilities to ensure that clean energy technologies and systems are inherently secure and resilient to cyber or cyber-physical threats.

Listed in Table 1 below are programs that federal agencies are planning or implementing in fiscal years 2024, 2025, and possibly beyond, to meet the objectives of the 2023 *Federal Cybersecurity Research and Development Strategic Plan*.

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 composed of over 1,000 active individual grants to hundreds of researchers and their academic institutions. Also, programs in the table vary substantially in their sizes and amounts 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

Agency Key Cybersecurity R&D Programs	**Protect People and Society**			**Establish Trust**	**Cyber Resilience**					**Federal Priority Application Scenarios**		
	Cybersecurity Through Human-centered Approaches	Empower Organizations to Tackle Cybersecurity Threats	Cybersecurity Education and Workforce Development	Establish and Negotiate Trust	Cyber Resilience by Design	Deter	Protect	Detect	Respond	Protect SW and HW Supply Chain	Realize Secure and Trustworthy AI	Secure Clean Energy Future
Air Force Research Laboratory (AFRL)												
Advanced Course in Engineering (ACE)			X									
Automated Vulnerability Identification Prioritization for Embedded Resources (A-VIPER)								X				
Basic Research	X		X	X	X	X	X	X	X		X	
Critical Infrastructure Resiliency and Prediction of Cascading Effects (CIRCAT)							X					
Estonia PA							X		X			
Fundamentals of Cyber Science (FoCS)						X	X	X	X			
Rapid Cyber Prototyping and Transition (RCPAT)							X	X				
Salient Ghost Phase 2								X				
T-CORE Processor				X	X	X	X	X	X	X		
Virtual Institutes for Cyber and Electromagnetic Spectrum Research and Employ (VICEROY)			X									
ARMY												
Adversarial Resilient Cyber Effects for Decision Dominance (ARCEDD)							X	X				
Camouflage						X	X					
Cyber Defense MURI											X	
Deception MURI						X						
Predictive Intelligent Networking (PIN) - Cyber							X				X	

Agency Key Cybersecurity R&D Programs	**Protect People and Society**			**Establish Trust**	**Cyber Resilience**					**Federal Priority Application Scenarios**		
	Cybersecurity Through Human-centered Approaches	Empower Organizations to Tackle Cybersecurity Threats	Cybersecurity Education and Workforce Development	Establish and Negotiate Trust	Cyber Resilience by Design	Deter	Protect	Detect	Respond	Protect SW and HW Supply Chain	Realize Secure and Trustworthy AI	Secure Clean Energy Future
PKI Modernization / Dynamic Access Control-Tactical				X			X					
Quantitative Measurement of Cyber Resilience (QMoCR)					X							
Tactical Autonomous Active Cyber Defense (TAACD)							X	X	X			
Tactical Hardening for Quantum (THfQ)				X			X					
Tactical Zero Trust (TZT)				X								
TrojAI											X	
Defense Advanced Research Projects Agency (DARPA)												
Business Process Logic (BPL)							X					
Carcosa						X						
Cyber Agents for Security Testing and Learning Environments (CASTLE)									X			
Constellation						X						
Enhanced SBOM for Optimized Software Sustainment (E-BOSS)										X		
Hardening Development Toolchains Against Emergent Execution Engines (HARDEN)					X							
Intelligent Generation of Tools for Security (INGOTS)								X				
Open, Programmable, Secure 5G (OPS-5G)							X					
Pipelined Reasoning of Verifiers Enabling Robust Systems (PROVERS)					X							

Agency Key Cybersecurity R&D Programs	**Protect People and Society**			**Establish Trust**	**Cyber Resilience**					**Federal Priority Application Scenarios**		
	Cybersecurity Through Human-centered Approaches	Empower Organizations to Tackle Cybersecurity Threats	Cybersecurity Education and Workforce Development	Establish and Negotiate Trust	Cyber Resilience by Design	Deter	Protect	Detect	Respond	Protect SW and HW Supply Chain	Realize Secure and Trustworthy AI	Secure Clean Energy Future
Signature Management using Operational Knowledge and Environments (SMOKE)						X						
Verified Security and Performance Enhancement of Large Legacy Software (V-SPELLS)					X							
Department of Energy (DOE)												
CESER RMT Cyber RD&D					X		X	X	X		X	X
CESER RMT Develop and Deploy		X										X
CESER RMT University-Based Cybersecurity Centers			X				X	X	X		X	X
Consequence-driven Cyber-informed Engineering (CCE)			X		X							X
Cyber-Informed Engineering (CIE)			X		X							X
Energy Cyber Sense										X		X
Clean Energy Cybersecurity Accelerator		X		X	X		X	X	X	X		X
Cybersecurity of DERS and EV Charging Infrastructure					X		X	X				X
CyOTE							X	X	X			
SecureNET		X	X	X								
Infrastructure Investment and Jobs Act (IIJA) Sec. 40125b Cybersecurity R&D			X				X	X	X		X	X
Department of Homeland Security (DHS)												
Center for Accelerating Operational Efficiency (CAOE)	X		X								X	

Agency Key Cybersecurity R&D Programs	**Protect People and Society**			**Establish Trust**	**Cyber Resilience**					**Federal Priority Application Scenarios**		
	Cybersecurity Through Human-centered Approaches	Empower Organizations to Tackle Cybersecurity Threats	Cybersecurity Education and Workforce Development	Establish and Negotiate Trust	Cyber Resilience by Design	Deter	Protect	Detect	Respond	Protect SW and HW Supply Chain	Realize Secure and Trustworthy AI	Secure Clean Energy Future
Criminal Investigations and Network Analysis (CINA)			X			X					X	
Critical Infrastructure Resilience Institute (CIRI)			X			X				X		
Critical Infrastructure Security & Resilience Research (CISRR)		X		X	X		X			X		
Cyber Analytics and Platform Capabilities (CAPC)		X			X		X	X	X		X	
Cyber Machine Learning							X	X	X		X	
Cybersecurity Threats Technology Center (CT-TC)	X						X	X	X	X	X	
Cybersecurity Training for Law Enforcement			X			X						
Data Analytics Technology Center (DA-TC)							X	X	X		X	
Natural Language Processing (NLP)									X		X	
Sensors & Platform Tech Center (SP-TC)							X			X		
Software Assurance & Data Protection								X		X		
National Institutes of Health (NIH)												
Modeling Cyber Attack Impacts on Patient Outcomes		X										
NIH Data Path			X									
NIH Bridge2AI											X	
Department of Defense (DOD) High-Performance Computing Modernization Program (HPCMP)												
Cybersecurity Enhancement Project (CSEP)							X	X	X			
Cybersecurity Environment for Detection, Analysis, & Reporting (CEDAR)							X	X	X			

Agency Key Cybersecurity R&D Programs	**Protect People and Society**			**Establish Trust**	**Cyber Resilience**					**Federal Priority Application Scenarios**		
	Cybersecurity Through Human-centered Approaches	Empower Organizations to Tackle Cybersecurity Threats	Cybersecurity Education and Workforce Development	Establish and Negotiate Trust	Cyber Resilience by Design	Deter	Protect	Detect	Respond	Protect SW and HW Supply Chain	Realize Secure and Trustworthy AI	Secure Clean Energy Future
Ecosystem for Cyber Analytics		X			X		X	X	X			
Operationalizing the Cybersecurity Framework (OCF)					X		X	X	X			
National Institute of Standards and Technology (NIST)												
AI Risk Management Framework											X	
Cyber Security Framework/Risk Management Framework							X					
Device integrity		X										
Encryption						X						
Human Centered Cybersecurity	X											
Information and Communications Technology Supply Chain Risk Management (ICT SCRM/171)										X		
Identity and access management (IDAM)				X								
National Cybersecurity Center of Excellence (NCCoE) Energy Sector												X
NCCoE Playbooks									X			
National Vulnerability Database								X				
Secure engineering					X							
Secure Software Development Framework (SSDF)					X					X		
US National Initiative for Cybersecurity Education (NICE)			X									
National Security Agency (NSA)												
5G and NextG cybersecurity		X		X			X					

Agency Key Cybersecurity R&D Programs	**Protect People and Society**			**Establish Trust**	**Cyber Resilience**					**Federal Priority Application Scenarios**		
	Cybersecurity Through Human-centered Approaches	Empower Organizations to Tackle Cybersecurity Threats	Cybersecurity Education and Workforce Development	Establish and Negotiate Trust	Cyber Resilience by Design	Deter	Protect	Detect	Respond	Protect SW and HW Supply Chain	Realize Secure and Trustworthy AI	Secure Clean Energy Future
Adaptive cyber deception						X	X					
Autonomous cyber defense						X		X	X			
Advancing Resilient Collaborative Adaptive AI-Enabled Systems (CA2IS)					X							
Cyberpsychology	X										X	
Cybersecurity collaboration center		X	X									
Data fusion and analytics						X					X	
Formal methods-based trust tools				X								
H/W Supply Chain Protections										X		
Human machine teaming for s/w analysis						X			X			
Realize secure and trustworthy AI				X							X	
Science of security			X									
SE-Linux policy							X					
Systems architecture analysis					X	X						
National Science Foundation (NSF)												
Cybersecurity Innovation for Cyberinfrastructure (CICI)	X	X		X	X	X	X	X	X			
Secure and Trustworthy Cyberspace (SaTC) Program	X	X	X	X	X	X	X	X	X	X	X	
Privacy-Preserving Data Sharing in Practice (PDaSP)	X	X		X	X		X	X	X	X	X	
Office of Naval Research (ONR)												
Autonomic Cyber Operations		X			X		X		X		X	
BotRaids		X				X			X			

Agency Key Cybersecurity R&D Programs	**Protect People and Society**			**Establish Trust**	**Cyber Resilience**					**Federal Priority Application Scenarios**		
	Cybersecurity Through Human-centered Approaches	Empower Organizations to Tackle Cybersecurity Threats	Cybersecurity Education and Workforce Development	Establish and Negotiate Trust	Cyber Resilience by Design	Deter	Protect	Detect	Respond	Protect SW and HW Supply Chain	Realize Secure and Trustworthy AI	Secure Clean Energy Future
Dominating Information using Stealthy Resilient Unblockable Protocol Transformations (DISRUPT)	X			X			X					
Dynamic Concept-Relevant Deception	X					X			X			
Foundation Models for Automatic Generation of Correct-by-Construction Co (FM-AGC3)				X			X				X	
HW Trojan Detection				X		X				X		
Integrity in DevOps							X	X		X		
Science of cyber warrior training	X		X									
Self-Healing Ships					X				X			X
Software Debloating	X	X					X			X		X
Office of the Under Secretary of Defense (OUSD)												
Accelerate Use of Intel ICX-D 3U VPX Security Enhancement				X			X					
Augmented Cyber Cognition with Operational Learning Automation of Deployable Expertise (ACCOLADE)						X	X	X	X		X	
Blue Phyzzing					X		X	X				
Integrated Non-Kinetic Force Development					X	X	X	X	X			
Pacific Intelligence and Innovation Initiative (P3I)			X									
University Consortium for Cybersecurity (UC2)			X									

Agency Key Cybersecurity R&D Programs	**Protect People and Society**			**Establish Trust**	**Cyber Resilience**					**Federal Priority Application Scenarios**		
	Cybersecurity Through Human-centered Approaches	Empower Organizations to Tackle Cybersecurity Threats	Cybersecurity Education and Workforce Development	Establish and Negotiate Trust	Cyber Resilience by Design	Deter	Protect	Detect	Respond	Protect SW and HW Supply Chain	Realize Secure and Trustworthy AI	Secure Clean Energy Future
Virtual Institutes for Cyber and Electromagnetic Spectrum Research and Employ (VICEROY)			X									