
# FY2020 FEDERAL CYBERSECURITY R&D STRATEGIC PLAN IMPLEMENTATION ROADMAP

Appendix to the Networking & Information Technology Research & Development Program Supplement to the President's FY2020 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

SEPTEMBER 2019

**About the National Science and Technology Council**

The NITRD Program is managed by the NITRD Subcommittee of the National Science and Technology Council (NSTC) Committee on Science and Technology Enterprise. The 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**

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 research and development (R&D) foundations for ensuring continued U.S. technological leadership and meeting the needs of the Nation for advanced IT. The National Coordination Office (NCO) 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. 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. 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 FY2020 implementation details for the 2016 Federal Cybersecurity Research and Development Strategic Plan. It lists key Federal projects and programs that directly contribute to solving the cybersecurity challenges outlined in the 2016 Federal Cybersecurity R&D Strategic Plan. This document accompanies the *NITRD Supplement to the President's FY2020 Budget Request*, available at https://www.nitrd.gov/pubs/FY2020-NITRD-Supplement.pdf.

**Copyright Information**

# FY2020 FEDERAL CYBERSECURITY R&D STRATEGIC PLAN IMPLEMENTATION ROADMAP

This document provides FY2020 implementation details for the *2016 Federal Cybersecurity Research and Development Strategic 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 FY2020 Budget*.[2]

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 *2016 Federal Cybersecurity Research and Development Strategic Plan*. The four strategic defensive elements of the strategic plan consist of Deter, Protect, Detect, and Adapt, as defined below:

- **Deter:** The ability to efficiently discourage malicious cyber activities by measuring and increasing the costs to adversaries who carry out such activities, diminishing their spoils, and increasing risks and uncertainty of consequences for cyber attacks.
- **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 perfect security is not possible and systems should be assumed to be vulnerable to malicious cyber activities.
- **Adapt:** The ability of defenders, defenses, and infrastructure to dynamically adapt to malicious cyber activities by efficiently reacting to disruption, recovering from damage, maintaining operations while completing restoration, and adjusting to be able to thwart similar future activity.

Listed in the roadmap table below are projects and programs being planned or carried out in fiscal years 2019, 2020, and possibly beyond, to meet the objectives of the *2016 Federal Cybersecurity Research and Development Strategic Plan*. The strategic plan provides priorities for cybersecurity R&D in alignment with the NIST *Framework for Improving Critical Infrastructure Cybersecurity*,[3] which provides guidance on managing and reducing cybersecurity risk confronted by businesses and organizations.

The programs and projects listed in Table 1 represent key agency activities in the four defensive areas, 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. Likewise, 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.

---

[1] https://www.nitrd.gov/pubs/2016-Federal-Cybersecurity-Research-and-Development-Strategic-Plan.pdf. An update to this plan is underway, with publication expected early in FY2020.

[2] https://www.nitrd.gov/pubs/FY2020-NITRD-Supplement.pdf

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

## Table 1: Federal Cybersecurity R&D Strategic Plan Implementation Roadmap

| Planned/Ongoing Federal Cybersecurity R&D Programs, by Agency | Deter | Protect | Detect | Adapt |
|---|---|---|---|---|
| **Air Force Research Laboratory and Air Force Office of Scientific Research (AFOSR)** | | | | |
| AFOSR basic research in cybersecurity and information assurance | X | X | X | X |
| Agile and Resilient Embedded Systems | | X | X | X |
| Automated Cyber Survivability | | X | X | X |
| Computational Diversity for Cybersecurity | | X | | |
| Cyber-Physical Information and Intelligence | | | X | |
| Nova: system vulnerability assessment | | X | | |
| Robust and Secure Systems | | X | | |
| Trusted and Resilient Systems | | X | X | X |
| **Army Futures Command Combat Capabilities Development Command; Army Research Laboratory; and Command, Control, Computers, Communications, Cyber, Intelligence, Surveillance, and Reconnaissance Center** | | | | |
| Agile Cyber Maneuver & Resilience | | | X | X |
| Autonomous Cyber | | X | | X |
| Camouflage and Decoy of CEMA (cyber and electromagnetic activities) for Network Survivability | X | | | X |
| Cyber Deception and Cyber Adaption Multidisciplinary University Research Initiative | X | X | | X |
| Cyber Research Alliance | X | | X | X |
| Decoy and Deterrence | X | | | X |
| Information Trust | | X | X | |
| State Change Anomalous Behavior Analysis for Radio Network Defense | | | X | |
| **Defense Advanced Research Projects Agency** | | | | |
| Active Social Engineering Defense | X | | | |
| Brandeis program | | X | | |
| Building Resource Adaptive Software Systems | | | | X |
| Computers and Humans Exploring Software Security | X | | | |
| Cyber Assured Systems Engineering | | X | | |
| Cyber Fault-tolerant Attack Recovery | | X | | |
| Cyber Hunting at Scale | | | X | |
| Dispersed Computing | | X | | |
| Enhanced Attribution | X | | | |
| Extreme DDoS (Distributed Denial of Service) Defense | | | | X |
| Harnessing Autonomy for Countering Cyber-Adversary Systems | | | | X |

**Table 1: Federal Cybersecurity R&D Strategic Plan Implementation Roadmap** (Continued)

| Planned/Ongoing Federal Cybersecurity R&D Programs, by Agency | Deter | Protect | Detect | Adapt |
|---|---|---|---|---|
| **Defense Advanced Research Projects Agency** (cont.) | | | | |
| Leveraging the Analog Domain for Security | | | X | |
| Rapid Attack Detection, Isolation and Characterization Systems | | | X | |
| SafeWare | | X | | |
| Space/Time Analysis for Cybersecurity | | X | | |
| Transparent Computing | | | X | |
| **Department of Defense High-Performance Computing Modernization Program (HPCMP)** | | | | |
| Cybersecurity Enhancement Project | | X | X | |
| Cybersecurity Environment for Detection, Analysis, and Reporting | | X | X | |
| HPC Architecture for Cyber Situational Awareness | | X | X | X |
| Information Security Continuous Monitoring—Jigsaw | | X | X | |
| Rapid Audit of Unix | | X | | |
| **Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response** | | | | |
| Cybersecurity for Energy Delivery Systems | | X | X | X |
| **Department of Homeland Security** | | | | |
| Commercial Accelerator Program | X | X | X | X |
| Cyber for Critical Infrastructure | | X | X | |
| Cyber Physical Systems | | X | X | |
| Next Generation Cyber Infrastructure | | X | X | |
| **National Institute of Standards and Technology** | | | | |
| Access control and privilege management | | X | | |
| Advanced security testing and measurement | | X | X | X |
| Biometric standards and testing | X | X | | |
| Cloud computing and virtualization | X | X | | X |
| Cryptographic standards, validation, and research (post-quantum cryptography, lightweight cryptography) | X | X | | |
| Identity management | | X | | |
| Information security risk management | | X | X | X |
| Internet infrastructure protection | | X | X | X |
| Machine Learning-based Anomaly Detection | | | X | |
| Mobile security | | X | | X |
| Privacy engineering | | X | | |
| Securing Artificial Intelligence | | X | | |

**Table 1: Federal Cybersecurity R&D Strategic Plan Implementation Roadmap** (Continued)

| Planned/Ongoing Federal Cybersecurity R&D Programs, by Agency | Deter | Protect | Detect | Adapt |
|---|---|---|---|---|
| **National Institute of Standards and Technology** (cont.) | | | | |
| Security and privacy of IoT (Internet of Things) | X | X | X | |
| Security of cyber-physical systems | | X | X | |
| **National Science Foundation** | | | | |
| Secure and Trustworthy Cyberspace Program | X | X | X | X |
| **National Security Agency** | | | | |
| Autonomous Cyber Defense | | | | X |
| Camo | | | X | |
| Centaur | X | | | |
| Boutique | X | | | |
| Data Fusion | | | X | |
| IoT Trust Anchors | | X | | |
| Mitigating Adversarial Machine Learning | | | X | |
| Radio-frequency identification (RFID) | | X | | |
| Security Enhancements–Internet of Things | | X | | |
| Secure Wearable Authentication Gear/Fast ID Online | | X | | |
| **Office of Naval Research** | | | | |
| Crypto Factory | | X | | X |
| HERCULE: Harmful Episode Reconstruction by Correlating Unsuspicious Logged Events | | | X | |
| MalSee | | | X | |
| Noise Factory | X | | | |
| Popcorn Linux | X | X | | |
| Resilient Hull, Mechanical, and Electrical Security | X | X | | X |
| Reverse Formal | X | X | | |
| Total Platform Cyber Protection Innovative Naval Prototype | | X | X | X |
| **Office of the Secretary of Defense** | | | | |
| Autonomous Cyber Defense | X | X | X | X |
| Autonomous Intelligent Resilient Security | | X | X | X |
| Autonomous Self-Securing Cyber Systems | | X | X | X |