FEDERAL CYBERSECURITY RESEARCH AND DEVELOPMENT STRATEGIC PLAN

A Report by the

CYBER SECURITY AND INFORMATION ASSURANCE
INTERAGENCY WORKING GROUP

NETWORKING AND INFORMATION TECHNOLOGY
RESEARCH AND DEVELOPMENT SUBCOMMITTEE

of the

NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

December 2023

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, 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 budgets and serves as a source of scientific and technological analysis and judgment for the President concerning 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 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 research and development strategies coordinated across federal agencies to accomplish 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 research and development 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 Cyber Security and Information Assurance (CSIA) Interagency Working Group (IWG) of the NITRD Subcommittee is focused on advancing solutions to many cybersecurity issues through coordination of federal cybersecurity research and development (R&D) investments and activities, including developing joint research strategies and engaging academia and industry through workshops and other outreach activities. CSIA IWG member agencies focus on federal R&D to protect information, information systems, and people from cyber threats. Such information systems provide critical functions in every sector of the economy, including in national defense, homeland security, and other vital federal missions. More information is available at https://www.nitrd.gov/groups/csia/.

About This Document

This 2023 Federal Cybersecurity Research and Development Strategic Plan supersedes the 2019 Federal Cybersecurity Research and Development Strategic Plan. The Plan aims to coordinate and guide federally funded R&D in cybersecurity, including development of consensus-based standards and best practices. This Plan identifies five priority areas (human-centered cybersecurity, trustworthiness, cyber resilience, cybersecurity metrics, and cybersecurity research infrastructure) and three federal priority application scenarios (secure software and hardware supply chain, trustworthy artificial intelligence, and secure clean energy future) as the focusing structure for federal cybersecurity R&D activities and investments to benefit the nation.

Copyright

Note: Any mention in the text of commercial, non-profit, academic, or other non-governmental entities or their products is for information only; such references are not intended to imply or directly indicate endorsement or recommendation by any U.S. Government agency or entity.

NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

Chair
Arati Prabhakar, Assistant to the President for Science and Technology**,** Director, Office of Science and Technology Policy

Acting Executive Director
Kei Koizumi, Principal Deputy Director for Policy, Office of Science and Technology Policy

SUBCOMMITTEE ON NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT

Co-Chair
Dilma Da Silva, Acting Assistant Director for Computer and Information Science and Engineering, National Science Foundation

Co-Chair
Craig Schlenoff, Director, National Coordination Office

CYBER SECURITY AND INFORMATION ASSURANCE INTERAGENCY WORKING GROUP

Co-Chair
Jeremy Epstein, Program Director, National Science Foundation

Co-Chair
Matthew Scholl, Chief, Computer Security Division, National Institute of Standards and Technology

Technical Coordinator
Tomas Vagoun, National Coordination Office for Networking and Information Technology Research and Development

Writing Team Members

Evan Austin, Naval Research Laboratory
Maruan Barakat, Department of Defense, Office of the Under Secretary of Defense for Research and Engineering
Cindy Bethel, National Science Foundation
Michael Collins, National Security Agency
Donald Coulter, Department of Homeland Security
Jeremy Epstein, National Science Foundation
Hsin Fang, National Institute of Standards and Technology
Neil Gerr, Defense Advanced Research Projects Agency
Jonathan Heiner, Air Force Research Lab
James Joshi, National Science Foundation
Glenn Lilly, National Security Agency
Fowad Muneer, Department of Energy
Tristan Nguyen, Air Force Office of Scientific Research
Jessica Yoo Perry, Department of Energy
Matthew Scholl, National Institute of Standards and Technology
Matthew Turek, Defense Advanced Research Projects Agency
Tomas Vagoun, National Coordination Office for Networking and Information Technology Research and Development
Isidore Venetos, Federal Aviation Administration
Cliff Wang, National Science Foundation

Table of Contents

1 Executive Summary

President Biden has been clear that cybersecurity is essential to the basic functioning of our economy, the operation of our critical infrastructure, the strength of our democracy and democratic institutions, the privacy of our data and communications, and our national defense. That's why the Biden-Harris Administration released the *National Cybersecurity Strategy* (NCS) in March 2023. The NCS makes it clear that advances in cybersecurity are urgently needed to prevent and thwart malicious activities and adversaries, insider threats, and to strengthen public trust in the digital ecosystem.

This 2023 *Federal Cybersecurity Research and Development Strategic Plan* (the Plan) provides federal agencies updated guidance on the overall priorities for federally funded research and development in cybersecurity. The guidance incorporates objectives from the NCS and establishes research priorities for developing the science and technology needed to advance the goals of the Biden-Harris Administration in cybersecurity. This Plan identifies the following objectives and critical dependencies:

- **Human-centered cybersecurity**: A greater emphasis is needed on human-centered approaches to cybersecurity where people's needs, motivations, behaviors, and abilities are at the forefront of determining the design, operation, and security of information technology systems.
- **Trustworthiness**: Capabilities are needed to be able to establish and enforce the required levels of trust at all layers of computing, starting at the hardware layer and including all other layers, such as operating systems, software applications, networking, web browsing, and applications and services such as electronic commerce and information sharing on social media.
- **Cyber resilience**: Capabilities are needed to ensure that systems can withstand cyberattacks and disruptions, and can continue to deliver vital functions in the face of impairment in adverse and contested cyber environments.
- **Cybersecurity metrics, measurements, and evaluation**: Advancements are needed in capabilities to evaluate and quantify cybersecurity risks, resilience, and trustworthiness, in a scientifically sound, technology-agnostic, and tailorable manner, for all levels of an organization and organization's products, supply chains, and operations.
- **Cybersecurity research, development, and experimentation infrastructure**: An up-to-date, national-level cybersecurity research, development, and experimentation infrastructure is needed to support innovation at the scope and scale of cyberspace and the speed of advances by adversaries.

The Plan also focuses on research priorities in the following Federal Priority Application Scenarios:

- **Protect software and hardware supply chain**
- **Realize secure and trustworthy artificial intelligence**
- **Secure the clean energy future**

The Plan closes with identifying roles in cybersecurity R&D for the federal government, industry, and academia, and approaches for coordination and collaboration. Implementing this Plan will create science and technology for cybersecurity to help sustain a trustworthy cyberspace to support the nation's prosperity and security.

2 Introduction

President Biden's 2023 *National Cybersecurity Strategy* (NCS)[1] re-affirms the critical importance of cybersecurity[2] and its essential role in "the basic functioning of our democracy and democratic institutions, the privacy of our data and communications, and our national defense." The NCS emphasizes that a prosperous future will depend on the cybersecurity and resilience of the underlying technologies and systems.[3] However, the structure of the digital ecosystem and its components remains prone to disruption or unintentional human-errors, vulnerable to exploitation, and is often co-opted by malicious actors. To address these deficiencies, the Biden-Harris Administration charts a path in the NCS calling for "fundamental changes to the underlying dynamics of the digital ecosystem, shifting the advantage to its defenders and perpetually frustrating the forces that would threaten it," with the goal of achieving a "defensible, resilient digital ecosystem where it is costlier to attack systems than defend them, where sensitive information is secure and protected, and where neither incidents nor errors cascade into catastrophic, systemic consequences."[4] Strategic research and development (R&D) investments by the federal government can significantly contribute to advances in cybersecurity, help secure the digital ecosystem, and ultimately, strengthen the U.S. economy and national security.

Through the NCS and its Implementation Plan,[5] the FY 2024[6] and FY 2025[7] *Research and Development Budget Priorities Memoranda*, the FY 2024[8] and FY 2025[9] *Administration Cybersecurity Budget Priorities Memoranda*, and the 2023 *National Cyber Workforce and Education Strategy*[10] the Biden-Harris Administration has established the following cybersecurity priorities:

- Rebalance the responsibility to defend cyberspace toward those that build and operate critical systems and the underlying technologies and lessen the burden on end users to mitigate cyber risks.
- Realign incentives and shape market forces to favor long-term investments in making cyberspace more resilient, defensible, and aligned with our values.
- Disrupt and dismantle threat actors and defend critical infrastructure.
- Forge international and commercial partnerships to pursue shared goals.
- Advance trustworthy, safe, secure, and privacy-preserving artificial intelligence (AI).
- Mitigate cybersecurity risks through security-by-design and resilience, strengthen security and resilience of critical infrastructure, and integrate social, behavioral, and economic research.

[1] https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

[2] https://csrc.nist.gov/glossary/term/cybersecurity

[3] Examples of systems include information systems, financial systems, manufacturing systems, transportation systems, logistics systems, medical systems, weapons systems, mechanical systems, space systems, industrial control systems. Systems can be physical or conceptual. https://doi.org/10.6028/NIST.SP.800-160v1r1

[4] https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

[5] https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf

[6] https://www.whitehouse.gov/wp-content/uploads/2022/07/M-22-15.pdf

[7] https://www.whitehouse.gov/wp-content/uploads/2023/08/M-23-20.pdf

[8] https://www.whitehouse.gov/wp-content/uploads/2022/07/M-22-16.pdf

[9] https://www.whitehouse.gov/wp-content/uploads/2023/06/M-23-18-Administration-Cybersecurity-Priorities-for-the-FY-2025-Budget-s.pdf

[10] https://www.whitehouse.gov/wp-content/uploads/2023/07/NCWES-2023.07.31.pdf

- Strengthen the cyber workforce and equip people with the education and skills needed to realize and protect the benefits of cyberspace.

In addition, the following executive and legislative actions help clarify the challenges and opportunities in cybersecurity: *Executive Order 14028: Improving the Nation's Cybersecurity*,[11] *Blueprint for an AI Bill of Rights*,[12] *CHIPS and Science Act of 2022*,[13] *Inflation Reduction Act of 2022*,[14] and *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*.[15] This 2023 *Federal Cybersecurity Research and Development Strategic Plan* (the Plan) considers the executive and legislative priorities, as well as the systemic, underlying deficiencies that cause cybersecurity vulnerabilities, and provides guidance and priorities for federal agencies that conduct or sponsor R&D in cybersecurity.

This Plan updates the 2019 *Federal Cybersecurity Research and Development Strategic Plan*[16] as required by the *Cybersecurity Enhancement Act of 2014*.[17] This law requires the National Science and Technology Council (NSTC) and the Networking and Information Technology Research and Development (NITRD) Program to develop, maintain, and update every four years a cybersecurity R&D strategic plan to guide the overall direction of federally funded R&D in cybersecurity.

This Plan was developed by a group of subject-matter experts from the Cyber Security and Information Assurance Interagency Working Group of the NITRD Program. Additionally, the group issued a federal Request for Information[18] through NITRD to provide industry, academia, and the public an opportunity to offer input to this Plan. Responses to this Request for Information are posted on the NITRD website.[19]

2.1 Purpose

The nation continues to face significant challenges in all areas of cybersecurity. The federal government has a unique role in cybersecurity R&D: it should drive fundamental change by investing in long-term basic research that can improve cyber safety and security for people, critical infrastructure, information, and the systems and networks that underpin cyberspace. Cybersecurity R&D is a shared responsibility between the government, industry, and academia. The government funds long-term, high-risk research, performs mission-specific R&D, and engages in targeted translational research. In contrast, industry funds research with near-term applications and transitions successful research into commercial products. Researchers and academia are entrusted with creating the knowledge and science that can create the foundations for secure and trustworthy solutions and technologies. This document lays out a research agenda for federally funded R&D carried out by government agencies and the U.S. R&D enterprise, informed by interactions with industry and academia.

[11] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[12] https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf

[13] https://www.govinfo.gov/content/pkg/PLAW-117publ167/pdf/PLAW-117publ167.pdf

[14] https://www.govinfo.gov/content/pkg/PLAW-117publ169/pdf/PLAW-117publ169.pdf

[15] https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/

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

[17] https://congress.gov/113/plaws/publ274/PLAW-113publ274.pdf

[18] https://www.federalregister.gov/documents/2023/02/07/2023-02578/request-for-information-on-the-2023-federal-cybersecurity-research-and-development-strategic-plan

[19] https://www.nitrd.gov/coordination-areas/csia/88-fr-10552-responses/

This Plan prioritizes and describes several research areas and capabilities that must be achieved to fundamentally improve cybersecurity. The Plan does not focus on specific technical problems, e.g., developing better intrusion detection systems or more secure operating systems. Rather, by describing desired capabilities, the priority areas reveal important underlying causes of cybersecurity vulnerabilities, and the potential impacts such vulnerabilities can have on the federal government mission and the overall health of the nation. Furthermore, by defining the desired capabilities, instead of what specific research to undertake, the priority areas invite a diversity of approaches and encourage innovation across disciplines and sectors.

This Plan carries forward these essential concepts and framing from the 2019 *Federal Cybersecurity Research and Development Strategic Plan*:

- Effective cybersecurity requires maturing competencies founded upon four defensive capabilities: Deter, Protect, Detect, and Respond.
- To improve cybersecurity practices, science and technology advances are needed in sustainably secure systems development and operation, in proactive risk management, and in demonstrating evidence of efficacy and efficiency of those practices.
- People, specifically users affected by computing and communication systems, must be protected by cybersecurity safeguards with the same, if not greater, urgency as systems, communications, and data.
- Frameworks and methodologies are needed that will enable developers to reason across and manage safety, security, resiliency, trust, and privacy requirements holistically and concurrently.
- Advances in scientific foundations, research infrastructure, and transition to practice are critical to successful cybersecurity R&D.

The following key updates and priorities are put forth by this 2023 Plan:

- **Human-centered cybersecurity**: Increasingly, cyberattacks exploit the roles, actions, unintentional errors, and propensities of humans, particularly as end users. A greater emphasis is needed on human-centered approaches for cybersecurity where people's needs, motivations, incentives, behaviors, and abilities are at the forefront of determining the purpose, design, operation, and security of information technology systems and solutions.
- **Trustworthiness**: A dearth of methods and mechanisms to determine the trustworthiness of an entity in cyberspace and to establish trust among interacting parties and components is a key shortcoming endemic to cyberspace. Capabilities are needed to establish and enforce the required levels of trust at all layers of computing, starting at the hardware layer and including all other layers (such as operating systems, software applications, networking) and services (electronic commerce, social media, etc.).
- **Cyber resilience**: There is a growing recognition that cybersecurity must go beyond the traditional focus on prevention, protection, and restoration to address the broader range of needs that organizations have when dealing with threats to their systems. Cyber resilience has emerged as a key element in the overall strategies for mission and business assurance. This necessitates increased attention to how systems can be effectively designed, developed, and operated to withstand cyberattacks and continue to operate at an appropriate level to carry out the mission in the face of ongoing attacks, or even when compromised.

3 Strategic Framing

3.1 Cybersecurity Context

Cybersecurity must be understood as a multifaceted and interdisciplinary domain where social, technical, economic, and legal needs and objectives interact. Solutions for improving cybersecurity need to be designed in this multidisciplinary context. This Plan is motivated by these observations and trends:

- Digital technologies are becoming more complex and intertwined with the activities of people, society, and physical environments. Cybersecurity incidents, both malicious and unintentional, can cause significant disruptions and harm to people, organizations, and society.
- Most cyberattacks exploit the actions and weaknesses of humans, especially as users of digital technologies. The growing complexity of cyberspace also increases the potential for human negligence and unintentional errors.
- It is primarily the users and the nation—not the creators of the technologies—who suffer the consequences of poor security.
- New digital technologies, both incremental and groundbreaking, are constantly introduced. These advancements place ever-evolving demands on the cybersecurity workforce, which struggles to make these technologies secure.
- As information systems grow in complexity, and as opportunities for their exploitation expand, establishing trust and ensuring trustworthiness become fundamental for establishing a secure cyberspace.

3.2 Desired Outcomes

The Federal Cybersecurity R&D Strategic Plan outlines a vision for the research needed to secure cyber systems and space today and into the future. The vision also lays the foundation for a scientific approach to address the cybersecurity challenges of tomorrow. This Plan seeks to achieve the following outcomes:

- Create a paradigm shift to cyber resilience, where cybersecurity, trustworthiness, and mission survivability are foundational design and operational considerations. Cyber resilience must be intrinsic to how a system is architected and managed, equal in importance to traditional considerations such as functionality and performance.
- Develop the means to effectively consider and incorporate human and societal needs, capabilities, and behaviors into the design, development, and operation of information systems and cyber resilience solutions.
- Evolve the digital ecosystem so that trustworthiness of entities and their interactions can be routinely and securely verified and assured.
- Increase the productivity of the cybersecurity workforce by: (a) improving access to innovative and state-of-the-art cybersecurity education and training; (b) effectively leveraging automation to accomplish low-level cybersecurity tasks; and (c) improving cyber resilience of information systems in a way that reduces demands on cybersecurity professionals.
- Develop techniques to quantify the value of cyber resilience and trust assurance so that they can be considered jointly with more traditional business objectives such as cost and time-to-market.

4 Cybersecurity Research Priorities

This section describes cybersecurity priority areas and corresponding objectives for research. This Plan focuses on key opportunities to make progress in cybersecurity by establishing priority areas for coordinated attention across the federal cybersecurity R&D enterprise.

Cybersecurity priority areas focus on a range of research domains to address a particular characteristic of the desired outcomes. Priority areas are interdisciplinary, necessitating innovations and contributions from many scientific and technological fields. Priority areas aim to solve multiple hard problems and provide a platform for collaboration with the private sector.

In addition, many specific scientific, socio-technical, and mission challenges require focused cybersecurity research. This Plan does not preclude such research and leaves the determination and implementation of such research to individual federal agencies and organizations.

The following subsections are organized with these elements:

- **Priority Area:** identifies key, high-level challenges and needs that should be addressed by cybersecurity research.
    - **Research Objectives:** describe specific research objectives within a priority area.
        - **Research Actions:** provide succinct descriptions of research deliverables that are expected to be accomplished to achieve a research objective.

4.1 Priority Area: Protect People and Society

The United States is committed to a vision of cyberspace that is open and secure, where the use of digital technologies protects and reinforces—not weakens—democracy, human rights, and fundamental freedoms, where individuals and organizations can trust the safety and the security of the digital technologies they rely on. That is the shared vision of the *Declaration for the Future of the Internet*,[20] launched by the Biden-Harris Administration with 60 partner countries from around the globe and by the Freedom Online Coalition,[21] a coalition of over 35 countries including the Unites States, a founding member of the coalition.

This shared global vision emphasizes that cybersecurity is not an end in itself, but rather the objective of cybersecurity is to protect people and society from intentional or unintentional harms possible through the use or misuse of digital technologies. This Plan envisions cybersecurity as a key enabler for a cyberspace that affirms and promotes human rights, fundamental freedoms, and prosperous societies.

Traditionally, cybersecurity has been approached through a technology-centric perspective, with limited consideration for people's needs, motivations, incentives, and behaviors. As a consequence, organizations have given emphasis to technological solutions (e.g., firewalls, intrusion detection systems) and have underprioritized a holistic understanding of the human-centered issues, including the needs,

[20] https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/28/fact-sheet-united-states-and-60-global-partners-launch-declaration-for-the-future-of-the-internet/

[21] https://freedomonlinecoalition.com/

choices, and motivations of people. As a result, a majority of cyberattacks exploit the roles and actions of people, particularly as end users.[22]

Human-centered approaches for cybersecurity are needed, which ask: security for whom, from what, for what purpose, and through what means, where people are considered as part of both the solutions and challenges.

4.1.1 Research Objective: Strengthen Cybersecurity Through Human-Centered Approaches

Human-centered approaches are considered an "interdisciplinary methodology of putting people, including those who will use or be impacted by what one creates, at the center of any process to solve challenging problems."[23] Such approaches incorporate participatory and iterative designs to address the needs of people, organizations, communities including marginalized and vulnerable populations, and society related to cybersecurity. This empowers people to be invested in the process and provides a locus of control to support and encourage them to be a part of the cybersecurity solutions created.

Human-centered approaches to cybersecurity require improved training for better understanding the needs of the people using digital technologies and systems. It is important to understand what aspects of cybersecurity people excel with and what aspects should be handled by digital technologies. There is a need to reduce the burden of cybersecurity requirements on people, organizations, communities, and society, and to improve the usability and the user experience of digital technologies and systems. Research on human-centered computing aspects has indicated that including end users early in the process of design and development creates more usable systems and an improved user experience.[24] By better understanding the needs and behaviors of users, systems can be designed to reduce security practice responsibilities that are placed on people.

Threats[25] are becoming more sophisticated, for example, through more convincing phishing (e.g., malicious/deceptive email or text messages) and vishing (e.g., malicious/deceptive calls or voicemail) approaches. It is becoming increasingly challenging for people to identify these types of threats. There needs to be an emphasis on the development of socio-technical solutions to detect such attacks and mitigate them without relying on people to identify these threats.

In addition to the increased focus on usable security, it is necessary to understand what is important to people and society as it relates to cybersecurity. People, organizations, and society are impacted by security breaches. There is a need to understand what people and society believe needs to be protected and secured. However, there is a scarcity of information on how to translate people's and society's needs, desires, norms, incentives, and rights related to cybersecurity into actionable approaches and constructs that can be implemented by system designers and developers. Human-centered validation of

[22] Estimates vary from about 70-90% depending on sources, definitions, and methodologies. See for example: 2023 Verizon Data Breach Investigations Report, https://www.verizon.com/business/resources/reports/dbir; ENISA Threat Landscape 2022, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022/.

[23] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/12/13/executive-order-on-transforming-federal-customer-experience-and-service-delivery-to-rebuild-trust-in-government/

[24] https://csrc.nist.gov/CSRC/media/Projects/usable-cybersecurity/images-media/Is%20Usable%20Security%20an%20Oxymoron.pdf

[25] A *threat* is a potential cause of unacceptable *asset loss* and the undesirable consequences or impact of such a loss. https://doi.org/10.6028/NIST.SP.800-160v2r1

these systems and cybersecurity approaches are needed to improve our understanding of whether the technologies or services support the needs of people, organizations, communities, and society.

Research Actions: Strengthen Cybersecurity Through Human-Centered Approaches

- Create innovative approaches to engage end users in the development of secure digital technologies, to build systems that support people and how they use these systems.
- Investigate what factors and practices of human-centered design support successful and secure user engagements with digital technologies.
- Identify factors associated with human-centered design that result in unsuccessful systems and obstacles for end users and other stakeholders of these systems.
- Develop approaches for including what people, organizations, communities, and society value and desire to be secured and protected in the design of digital technologies.
- Demonstrate how the needs of people, organizations, communities, and society can be effectively considered in the design of solutions and practices that can mitigate cybersecurity threats and create positive user experiences.
- Study and model best practices for the validation of security properties of digital technologies in ways that include people who use and are impacted by these systems, ensuring usability, inclusivity, regulatory compliance, and a positive user experience.
- Identify factors that reduce or eliminate memory and cognitive loads of people who interact with digital technologies to ensure the safety and security of people and systems.
- Develop approaches to assess the impacts of cybersecurity solutions on people and society to understand if they are effective, efficient, usable, inclusive, and create a good user experience.
- Validate design and programming processes, procedures, behavioral cues, and other methodologies for supporting end users engaging in positive, security-minded actions.

4.1.2 Research Objective: Empower Organizations to Tackle Cybersecurity Threats

Organizations struggle to address the dynamic nature of cybersecurity threats.[26] It is difficult and costly to create an infrastructure capable of dynamically maintaining an organization’s strong security posture. It is important to develop assessment methods that support organizations regardless of size so that they can determine their security risks, vulnerabilities, and potential impacts on their assets, operations, and people.

4.1.2.1 Advance Cybersecurity Risk Analysis Methods

Cybersecurity risk analysis is a key part of effective risk management and facilitates decision-making at all levels of an organization. Mission and business objectives provide the context to conduct risk analysis, establish risk tolerances, and set expectations regarding risk management. These expectations provide cybersecurity risk analysis practitioners with the objectives necessary for managing cybersecurity risks. These objectives include identifying, mitigating, accepting, and/or monitoring risks to an organization.

However, most cybersecurity risk analysis frameworks are not sufficiently formalized, nor comprehensive. For instance, most frameworks rely on the use of risk matrices as their main analytic tool, utilizing ratings (likelihood, severity, and risk) that are prone to ambiguity and subjective interpretation. Moreover, those frameworks typically do not consider the intentionality of certain threats

[26] https://www.cisa.gov/topics/cybersecurity-best-practices/organizations-and-cyber-safety

and tend to produce comparable rating to risks that may be very different qualitatively, potentially resulting in suboptimal cybersecurity controls and resource allocations. In general, cybersecurity risk analysis faces the challenge of a lack of reliable and accountable methods, and is further complicated by the fact that threats, threat vectors, and vulnerabilities change as adversaries evolve.

Cybersecurity risk analysis is a core component for the overall goal of risk management, and there are R&D challenges with respect to effective, repeatable, and useable cybersecurity risk assessments.

Research Actions: Advance Cybersecurity Risk Analysis Methods

- Develop techniques to assess the formality, rigor, outcomes, and benefits of risk analysis methods, including their applicability in different organizations and enterprises.
- Identify the limitations of the specific analysis, assessment, and aggregation methodologies, tools, and techniques employed in cybersecurity risk analysis, including the subjectivity and quality of the data used.
- Develop more comprehensive frameworks for cybersecurity risk management, for example, by incorporating additional information about adversaries through an adversarial risk analysis, and by incorporating financial risk mitigations through methods such as cyber insurance.
- Identify approaches and techniques for automating cybersecurity risk analysis at scale to make it effective, affordable, and accessible to many risk audiences.
- Investigate the application of economics to cybersecurity risk analysis and management, including concepts such as game theory, network externalities, asymmetric information, moral hazard, and the tragedy of the commons.
- Develop approaches that can ensure that cybersecurity risk analysis is composable and quantifiable in the context of overall enterprise risk faced by organizations to improve understanding of cybersecurity risks across multiple levels of an organization.
- Create risk quantification and data to allow for cybersecurity investment, technology, and architecture decisions at operational and strategic levels of organizations.
- Develop methods for standardization, integration, and anticipation of threat actions to inform risk analysis in actionable, effective, and forward-looking decisions.

4.1.2.2 Explore Cybersecurity Markets and Approaches to Incentivize and Require Good Cybersecurity Practices

Market structures, incentives, and disincentives can help establish the cost/benefit conditions that favor effective cybersecurity practices and their positive effects for people, organizations, and society in both the long term and short term.[27] There is a need to better understand what market structures and what types of incentives will support improved cybersecurity practices and outcomes. Solutions exist to counter many threats and vulnerabilities; however, those solutions are not widely used since incentives for their use are typically not aligned with objectives, and resources are not correctly allocated. Sound economic incentives need to be based on sound metrics, sensible and enforceable notions of liability, and mature cost-benefit risk analysis methods.

Practical and policy questions that call on economics research include how to incentivize investments in cybersecurity by private organizations and persons, and how to understand the costs and benefits of

[27] https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

cybersecurity interventions in a world lacking objective metrics of risk and damages from breaches of security, privacy, and the effect of misinformation on people. Research to understand and mitigate these problems includes fundamental economics research to better understand the security of data markets, digital assets, and supply chains. It also includes interdisciplinary research on how people, organizations, and governments value and make decisions on cybersecurity, privacy, and information integrity (including the economic aspects of regulation and regulatory behavior). Additionally, applied economics research should be conducted on the role of economic incentives in the growing foreign and domestic threats to information integrity.

Research Actions: Explore Cybersecurity Markets and Approaches to Incentivize and Require Good Cybersecurity Practices

- Explore and identify what market structures, liabilities, types of incentives (and disincentives), and requirements would ensure better cybersecurity outcomes for people, organizations, communities, and society.
- Identify objective metrics that could be used to determine cybersecurity and privacy risks for different stakeholders, populations, and vulnerable groups.
- Explore approaches that industry could use to insure against and/or limit the risks of cybersecurity and privacy breaches and violations.
- Develop approaches to determine the costs of cybercrime, cyber-deceptions, and harmful information manipulation to victims, affected organizations, insurers, and to the justice infrastructure (police, courts, prisons, etc.).
- Develop methodologies and metrics to understand the broader costs of cybersecurity incidents, including those that propagate among industries. Explore how those dependencies could be leveraged to spur cooperation and investments in cyber resilience by multiple industries.
- Identify approaches for designing economically efficient, effective, and incentive-compatible cybersecurity regulation.
- Examine how different actors in the cybersecurity ecosystem enhance or hinder innovation.

4.1.3 Research Objective: Strengthen Cybersecurity Education and Leverage AI-Powered Automation

Meeting the demand for skilled cyber workers is an urgent concern, with studies indicating shortages of hundreds of thousands of cybersecurity professionals.[28] Significant efforts by the federal government have been devoted to cybersecurity education and workforce development, such as the National Science Foundation's (NSF) CyberCorps® Scholarship for Service[29] program, National Institute of Standards and Technology's (NIST) NICE[30] program, National Security Agency's (NSA) National Centers of Academic Excellence in Cybersecurity[31] program, and Cybersecurity and Infrastructure Security Agency's (CISA) programs.[32]

[28] https://www.whitehouse.gov/wp-content/uploads/2023/07/NCWES-2023.07.31.pdf
[29] https://new.nsf.gov/funding/opportunities/cybercorps-scholarship-service-sfs-0
[30] https://www.nist.gov/itl/applied-cybersecurity/nice
[31] https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/
[32] https://www.cisa.gov/topics/cybersecurity-best-practices/cybersecurity-education-career-development

Agencies should continue to accelerate cybersecurity workforce capacity building, including funding research efforts for improving and evaluating efforts in K-12, higher education, and workforce training that result in increased skills and interest by students and people in cybersecurity. There is a need to accelerate the development of relevant and effective curricula and innovative education methodologies for different levels of students and workforce. It is also important to develop and provide appropriate training and support to educators at all levels. Additionally, effective approaches and incentives should be developed to fill U.S. Government positions. Furthermore, the rapid adoption of AI and automation raises a critical need for cybersecurity education to address how AI will affect both future cybersecurity work and people's everyday interactions with technology.

The significant extent of the unmet demand for cybersecurity professionals is an indication of both the growth and importance of information technologies (IT) in many sectors of the U.S. economy (and worldwide). It also suggests that the IT industry is developing and fielding systems and technologies that are not secure, requiring significant efforts by the cybersecurity workforce to secure them after they have been introduced. Cybersecurity education and training must drive a change in how information technologies and systems are designed and operated to help achieve a paradigm shift, where security is built in and cyber resilience is among the principal value propositions and management objectives of those technologies and systems.

The cybersecurity workforce needs to be able to better leverage automation to accomplish low-level cybersecurity tasks. This requires an improved understanding of what cybersecurity tasks can be delegated to automation, particularly AI-based, and what tasks require or can be better performed by people. This also requires changes in cybersecurity education to train students and practitioners in using, developing, and assessing AI systems to achieve the desired automation. Furthermore, cybersecurity practitioners must also understand the risks of using AI and automation, vulnerabilities of AI systems and how they might be compromised, and the use of AI by attackers.

To improve security and digital awareness of everyday users, cybersecurity education must go beyond the security professionals. There is limited research on how human-centered cybersecurity education and public awareness should account for the impact of AI technologies. Social engineering is one of the biggest threats. (Social engineering is a type of attack that manipulates a person into taking some action that leads to a successful cyberattack. For example, phishing (the use of malicious/deceptive emails or text messages), vishing (the use of malicious/deceptive voicemails), or the use of manipulated images such as deepfakes.) Attackers are increasingly able to use AI to create more believable and less detectable social engineering attacks. Most users of digital technologies have little knowledge of these risks. Bridging this gap for everyday users remains one of the major research challenges for cybersecurity education and workforce development.

Research Actions: Strengthen Cybersecurity Education and Leverage AI-Powered Automation

- Investigate methods to embed a security mindset into cybersecurity curricula design practices from inception to deployment (for example, security should be taught from the first programming class to capstone projects; or memory-safe programming languages and similar security-by-design constructs should be introduced early in the curriculum).
- Develop models and methodologies that can be used to determine the best way to utilize automation for low-level cybersecurity activities to empower the workforce to focus on higher-

level cybersecurity activities more suited for humans (or where people should not be taken out of the loop).
- Advance cybersecurity education and training to prepare workforces to utilize AI to improve cybersecurity and to mitigate potential AI-enabled threats.
- Develop best practices to include education and training in the ethical implications of using AI and assessing the risk associated with the utilization of AI approaches.
- Investigate methods, models, and best practices that leverage AI-powered automation to ensure systems, data, and communications are protected and secure.
- Identify effective interventions and incentives needed to inspire a subset of the cybersecurity workforce to invest in themselves and enter an "advanced" workforce that includes research and development professionals and educators.
- Study approaches for increasing diversity, equity, inclusion, and accessibility in cybersecurity education, workforce development, and community outreach in ways that encourage participation of people from all backgrounds, capabilities, and levels of knowledge.
- Expand approaches to support experiential learning, such as apprenticeships, internships, job-shadows, and other employer-educator partnerships, to align curriculum with workplace demands.
- Identify effective models to educate individuals of different backgrounds and ages to protect themselves from cyber threats and information manipulation on the internet.

4.1.4 Research Objective: Support Cybersecurity Policy Development

As put forth in the NCS, cybersecurity regulations and authoritative cybersecurity requirements have an important role in supporting national security and public safety. For example, Strategic Objective 1.1 of the NCS calls for establishing and harmonizing cybersecurity regulations to secure critical infrastructure, in a manner that corresponds to risks, reduces duplication, and is cognizant of the cost of implementation. In developing such regulations and requirements, it is important that policymakers leverage sound research from the science and technology community to make evidence-based and scientifically informed policy decisions. These policies will govern the way that government agencies operate and interact with private industry and the public, providing incentives for increased innovation while identifying guardrails to mitigate potential harm. The opportunities and risks that accompany technological developments are even more complex when their interconnectedness is considered, which necessitates an interdisciplinary, multi-perspective approach to establishing effective policies.

In another example, recent advances in AI require thoughtful and measured policy around the cyber resiliency of the technology itself, the near adjacent domains where AI can be applied, and the potential impacts across the government and society. The need to leverage data to build more effective machine learning (ML) capabilities has significant privacy, security, and potential bias implications, especially when these algorithms are leveraged for diverse use cases such as federal law enforcement and digital service delivery to citizens. Furthermore, the human-centered approach in developing the new capabilities and policies can ensure that cyber and AI policies are complimentary and not conflicting.

Advances in cybersecurity present new opportunities to increase trust and cyber resiliency in the systems and critical infrastructure upon which the nation depends. Cybersecurity research initiatives that expand knowledge and advance the technical basis must be complemented by active collaboration among researchers, policymakers, and practitioners to provide policymakers and practitioners with the information needed to make informed decisions about policy and technology, and to ensure that researchers have the real-world context necessary to discover novel approaches that yield desirable effects.

Research Actions: Support Cybersecurity Policy Development

- Identify effective approaches that holistically consider the needs and responsibilities of people, organizations, society, and the government, which will lead to the development of effective cybersecurity policies.
- Identify factors in priorities, incentives, and communication styles between researchers and policymakers that lead to important research remaining unknown to policymakers and practitioners.
- Develop methods and tools based on risk analysis, game theory, agent-based modeling, and other innovative approaches that would allow researchers and policymakers to explore a wide range of policy options. Pursue efforts to translate the findings of fundamental R&D into actionable recommendations for policymakers.
- Devise strategies to embed formal evaluation of policies and practices into their initial development, so that it is possible to continuously track the impacts and implications of regulations, policies, and practices related to cybersecurity from the start.
- Develop methodologies for including assessments of potential consequences and implications of regulations, policies, and practices, whether intentional or unintentional, as part of formal evaluations to help improve the efficacy of the policy- or practice-based approaches.
- Identify ways to increase the percentage of research efforts in which policy experts participate in research design and evaluation.

4.2 Priority Area: Develop Means to Establish and Manage Trust

Trust is a multidisciplinary topic with different disciplines such as sociology, economics, psychology, organization management, computing, and networking defining it in their own ways. For the purposes of this Plan, *trust* is considered to mean “a belief that an entity meets certain expectations and can be relied upon,”[33] and *trustworthiness* represents “objective trust based on observed outcome”[34] or a demonstrated ability based on verifiable evidence that the entity can be trusted to satisfy expectations.[35]

Trust and trustworthiness are foundational elements that are critical to ensuring safe and secure cyberspace. Today, cyberspace is composed of technologies and services that generally lack mechanisms to ascertain their security conditions and their trustworthiness. The dearth of mechanisms to determine the trustworthiness of an entity and establish trust among participating parties and components has made cyberspace less secure and more vulnerable to illicit exploitations and unintentional errors. Capabilities are needed to establish and enforce the required levels of trust at all layers of computing. The layers of computing include the hardware layer, operating systems, software, networking, web browsing, applications, and services such as electronic commerce, information sharing on social media, and interactions of people in the digital ecosystem. Such trust establishment includes ensuring the security of the technical foundations of the internet.

[33] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1r1.pdf
[34] https://dl.acm.org/doi/pdf/10.1145/2815595
[35] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1r1.pdf

All parties or components in a transaction or workflow must be able to agree on the level of trust, which should be enforced by the underlying infrastructure or achieved by formal guarantees. Research is needed to develop capabilities to articulate and negotiate situation-aware and mission-driven security requirements at hand, to adjust the assurance level on specific security attributes separately, and to establish and manage dynamically evolving trust between systems based on verifiable information. Trust between interacting components and parties, based on verifiable assertions and information, is the necessary condition for a secure and trustworthy cyberspace.

Research focused on trust has been explored in many areas including network services, peer-to-peer systems, multi-agent systems, mobile and wireless networks, cloud computing, Internet of Things (IoT) environments, social networks, reputation systems, etc. The highly multidisciplinary nature of trust management requires one to consider many contextual factors, trust attributes (e.g., attributes related to individual entities or relationship among them), various trust components (e.g., trust related to communication, information, and human factors), as well as various properties (e.g., subjectivity, asymmetry, or transitivity),[36] and the resulting complexity make trust and trust management a highly challenging area. In particular, R&D is needed to establish a robust science of trust to address challenges in the rapidly evolving multidisciplinary cybersecurity landscape to ensure that trust and trustworthiness can be continuously assessed, measured, and updated. Such foundational R&D should focus on trust modeling, methodologies, and frameworks to compose, assess, and verify trust and technologies to establish and maintain the desired trust relationships in highly dynamic environments. Ultimately, solutions are needed for establishing flexible, adaptive, composable, distributed trust relationships and environments that can support a wide range of functional and policy requirements and social contexts, in the face of evolving threats.

4.2.1 Research Objective: Develop Trust Models for Management of Identity, Access, and Interoperation

Foundational to building trustworthy cyberspace is to establish mechanisms to ensure that the identity of an entity in cyberspace can be verifiably trusted in any given interaction, situation, or mission. Identity trust is important in ensuring the appropriate access to computing or networking resources and systems and in ensuring the validity of the entities' interactions in establishing trusted exchanges with other entities. Such entities could be users, devices, individual systems or components, distributed systems, networks, or composed systems forming complex systems of systems.

It is important to accelerate research to design and develop comprehensive digital identity solutions to provide the foundation of trust in cyberspace. Research should explore digital identity approaches utilizing various identity attributes related to users and digital entities. Various authentication techniques including distributed or decentralized approaches and biometrics should be explored in different application contexts, including in emerging environments such as augmented or virtual reality and digital assets. Large scale digital identity infrastructures should also be explored to support the establishment and assessment of varying levels of dynamically evolving trust based on varying identity attributes and contexts. Such identity solutions may need centralized or decentralized trust evaluation, and efficient and scalable verification mechanisms to be carried out at scale. For example, a national-scale digital

[36] https://dl.acm.org/doi/pdf/10.1145/2815595

identity ecosystem may need extensive infrastructure support to manage keys and cryptographic protocols in an efficient and scalable manner.

Research is needed to advance trust-based, situation-aware, or mission-driven access and entity interactions. Such solutions should consider how to efficiently capture and specify access and interaction requirements from users, organizations, and regulatory/legal mandates, and devise efficient and scalable enforcement mechanisms.

Research Actions: Develop Trust Models for Management of Identity, Access, and Interoperation

- Identify attributes, factors, and contextual conditions or constraints that are needed for establishing trust in a variety of computing, networking, user or application contexts and technologies, including operations technologies that interact with physical environments.
- Develop foundational models of trust that can capture its dynamic nature, so that the security posture of entities, components, and systems, and interactions among them can be understood at any given time, and on a continuous basis.
- Develop metrics and measurement techniques for trust. Both quantitative and qualitative metrics, as well as computational approaches should be explored for computing, assessing, and verifying the trust posture of entities and interactions under consideration. How transitivity supports trust measurements within different contextual or mission requirements is an important research area.
- Advance digital identity methods that can utilize a variety of attributes related to users, entities, and systems, where varying levels of dynamic trust can be continuously assessed. Various authentication techniques, including distributed or decentralized approaches, that are efficient and scalable should be explored.
- Explore approaches for compositional trust, to be able to determine the trustworthiness of systems that contain components with varying levels of trust, have a diverse set of trust dependencies or transitivity properties, and engage in a variety of situation-aware or mission-driven interactions.
- Develop policy specification frameworks that efficiently integrate trust-based, dynamic, situation-aware or mission-driven access and usage control requirements, as well as assessments of trust of the entities involved.
- Design compositional frameworks that enable trust based, policy-governed secure interactions between different systems with diverse security and privacy requirements.

4.2.2 Research Objective: Develop Capabilities to Negotiate Trust

System interoperation at various levels is a common objective in today's cyberspace. Interoperation needs vary from transient, loosely coupled environments to tightly coupled or federated systems. Organizational trust, trust and assurance of individual systems and users, business relationships between organizations, and collaborative missions are among the critical factors in establishing interoperation among systems and infrastructures from multiple organizations. Trustworthy interoperation requires capabilities that can provide policy articulation, negotiation of dynamically evolving security attributes or context related to information sharing and interoperation, and requisite verifications and assurances necessary to establish varying levels of trust between components and systems. Additionally, trustworthy interoperation must be supported by robust enforcement of secure interoperation policies including the use of secure separation and isolation techniques (e.g., trusted execution environments) for protecting data-in-use, securing cross-domain information sharing and flow, as well as securing execution of distributed workflows and transactions that span multiple domains or jurisdictions.

It is important to explore foundational trust architectures such as zero-trust, or decentralized trust architectures that are scalable and efficient, and incorporate various dynamic trust models and metrics that may be appropriate for diverse infrastructures or scenarios (e.g., cloud-edge-IoT environments, operational technologies and critical infrastructures, health information exchanges, digital assets ecosystem, networks, service-oriented architectures) or applications (e.g., healthcare, supply chain, energy). Such research should address effective, continuous, real-time monitoring, assessment and re-evaluation of dynamic trust that is integrated with adaptive mitigation techniques.

Research Actions: Develop Capabilities to Negotiate Trust

- Identify what assurances or affordances are needed to establish trust, at various layers of computing and applications (i.e., at the hardware, networking, software, and applications layers, as well as information exchanges among people).
- Design models and frameworks to enable secure information flow and dynamically evolving trust among multiple systems or organizations building on the trustworthiness of the interoperating systems, entities, and environments.
- Develop a framework to achieve trust through assurances or affordances. The framework should enable system developers or owners to perform a real-time evaluation of assurance and affordance arguments and the supporting body of evidence to establish confidence in system components.
- Develop negotiation techniques, including automated ones, to support systems or organizations in establishing trust between them to facilitate system interoperation, cross-domain information flow, and collaboration. Multidisciplinary research that includes economics, computing and information, and law should be considered.
- Explore robust and scalable recommendation systems and approaches to build trust that governs interoperation and interactions among un-trusted entities or organizations in dynamic and potentially automated ways.

4.2.3 Research Objective: Develop Solutions to Sustain Trustworthy Information Ecosystems

Being able to establish and maintain information trust is also necessary for well-functioning information ecosystems where information manipulation is prevented or minimized, where learning, open exchange of ideas among people, healthy debate, and freedom of expression can thrive. Manipulated information can have destabilizing and harmful consequences for national security, democratic processes, economy, and safety at home and abroad. Harms associated with manipulated information affect people of all ages, nationalities, genders, racial backgrounds, and creeds. Recognizing the wide array of risks and potential harms and the importance of maintaining trustworthy information ecosystems, the White House released the *Roadmap for Researchers on Priorities Related to Information Integrity Research and Development* (Roadmap for IIRD).[37] The Roadmap for IIRD establishes objectives for federally funded information integrity R&D and provides a structure for coordinating R&D in related areas.

[37] https://www.nitrd.gov/pubs/Roadmap-Information-Integrity-RD-2022.pdf

Identifying trustworthy information and sustaining trustworthy information ecosystems depends significantly on being able to establish trust about the information, its sources and flow channel, and the purpose of its creation and dissemination. Here, trustworthy information is accurate, reliable, verifiable, linkable to the original source, and understandable. In trustworthy information ecosystems, people and organizations can effectively communicate the best information, in which threats to information trust or integrity are proactively addressed, and where individuals are able to move toward trustworthy conclusions about the quality, correctness, and intent of information they encounter.

From the cybersecurity perspective, information exchange among people within an information ecosystem is one of a number of communication layers that needs to be secured where capabilities are needed to articulate, establish, and verify varying levels of trust among the components and participants.

The following research priorities, adopted from the Roadmap for IIRD, focus on research priorities related to the information trust aspects of sustaining trustworthy information ecosystems.

Research Actions: Develop Solutions to Sustain Trustworthy Information Ecosystems

- Characterize, explain, and model the interaction of entities, threats and harms, processes, and technologies that affect trustworthiness of information and information flows, including the psychological, behavioral, and cultural aspects.
- Identify factors and assess their influence on persuasiveness of information manipulation, people's susceptibility to information manipulation, and people's resilience to information manipulation.
- Develop reliable methodologies to measure persuasiveness of manipulated information and how it affects cognition, beliefs, decision making, and behavior.
- Develop methodologies to assess the causal chain between information manipulation techniques, effects on people, and potential countermeasures and safeguards.
- Identify factors that affect the practicality or effectiveness of safeguards, including, but not limited to, platform design elements, characteristics of individuals or organizations, information sources, or threat actors.
- Investigate what affects people's assessment of trustworthiness and the properties that information flow paths/channels must have to be trusted by a wide variety of people.
- Develop approaches to model and analyze trust dynamics, dependencies, and trust transitivity characteristics to ensure appropriate information trust assessment.
- Develop forensic and provenance-based techniques for detecting information manipulation across a variety of media formats and platforms.
- Design approaches and technologies that help communities foster trust and productive discourse, especially for topic areas characterized by uncertainty, complex risk-benefit trade-offs, or lack of ground truth.

4.2.4 Research Objective: Enhance Trustworthiness of Cyberspace by Minimizing Privacy Risk and Harms

Trust in cyberspace has been significantly hampered by continuous cases of identity theft and privacy violations. Privacy violations can occur because of cybersecurity incidents or when privacy protection techniques are compromised. Establishing trust in cyberspace is critically dependent on ensuring that cybersecurity and privacy safeguards can adapt to the threat environment and minimize privacy risks of both intended and unintended harms, particularly to vulnerable groups and communities. Conversely, trust-based mechanisms that build on research outlined earlier in this section can bolster privacy mechanisms to ensure minimizing risks and harms. The R&D priorities presented in the *National Strategy to Advance Privacy-Preserving Data Sharing and Analytics*,[38] provide some key challenges related to privacy that should be addressed.

Research Actions: Enhance Trustworthiness of Cyberspace by Minimizing Privacy Risk and Harms

- Build policy frameworks to support specification and enforcement of privacy protection requirements while sharing or processing data, considering issues such as consent-and-notification, data confidentiality and data-in-use control, users' privacy desires or preferences, and privacy leakage through various means such as side channel leakage and inference attacks.
- Develop approaches for using trust models to strengthen privacy safeguards and minimize attack surfaces, risks, and harms.
- Extend policy-based approaches to capture trust-based security, privacy, and resilience requirements in an integrated way, while addressing potential tension or conflict between these different protection goals.
- Effective verification and validation techniques are needed to assess the privacy protection mechanisms that include both cryptographic (e.g., secure multiparty computation, zero knowledge proof, homomorphic encryption) and other techniques (e.g., based on statistics and information theory, Trusted Execution Environments).
- Develop trust modeling approaches that can assess trustworthiness of privacy solutions based on how they ensure privacy-utility tradeoffs, or based on the strength of privacy protection under various threat models.
- Develop multidisciplinary approaches to address social or human factors in capturing privacy desires and preferences, and to ensure that these are captured and verifiably enforced in the systems as expected.
- Expand trust modeling to assess assurance related to flow of privacy-sensitive information through various ecosystems such as advertising ecosystems, social networks ecosystems, and digital/crypto assets ecosystems.
- Explore research to establish trust through transparency and accountability solutions that complement or are part of privacy solutions.
- Develop privacy-auditing techniques to evaluate trustworthiness of privacy preserving technologies.

4.3 Priority Area: Strengthen Cyber Resilience

Resilience is generally defined as the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions including deliberate attacks, accidents, or naturally occurring threats or incidents.[39] Cyber resilience is the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by

[38] https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Strategy-to-Advance-Privacy-Preserving-Data-Sharing-and-Analytics.pdf

[39] https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf

cyber resources.[40] Cyber resilience enables mission or business objectives that depend on cyber resources to be achieved in a contested cyber environment. Cyber resilience can be a property of a system, network, service, system-of-systems, mission or business function, organization, critical infrastructure sector, sub-sector, region, or nation.

Historically, cybersecurity has largely focused on the prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authenticity, confidentiality, and non-repudiation.[41] However, there is a growing recognition that cybersecurity must go beyond prevention, protection, and restoration to address the broader range of needs that organizations have when dealing with threats to their systems. As the dependency on organizational systems for mission success increases, those systems must be trustworthy, secure, and resilient.

Cyber resilience emerged as a national priority in 2013 with the *Presidential Policy Directive 21 (PPD-21) on Critical Infrastructure Security and Resilience*.[42] More recently, the NCS and *CISA's 2023-25 Strategic Plan*[43] also prioritize cyber resilience as one of the principal objectives for the development of cyber solutions and technologies. Cyber resilience is emerging as a key element in any effective strategy for mission assurance, business assurance, and/or operational resilience.

The following sections discuss research priorities for achieving cyber resilience through foundational research, design, and operation.

4.3.1 Research Objective: Advance Science of Cyber Resilience

Cyber resilience is a multi-faceted concept that involves technology, people, and organizations. There are a number of disciplines such as computer science, systems engineering, statistics, social and behavioral sciences, organization and management sciences, and economics that contribute methods, processes, and solutions to understanding and achieving cyber resilience. A scientific challenge for strengthening cyber resilience is integrating relevant models and methods to capture interdependencies in the system, identify the salient causal relationships, and devise effective and efficient techniques, processes, and technologies to achieve the desired resiliency outcome.

Multi-scale models are needed to capture complex system dynamics, the effects of rapidly evolving threats, the effects of mitigation and restoration capabilities, and the dynamic impacts on the abilities of systems, people, and organizations to maintain desired functions and outcomes. Several cyber resilience frameworks have been introduced.[44,45,46,47] However, at this time, combining descriptive features with explanatory and predictive capabilities remains a challenge. Descriptive frameworks require theory to progress from disjointed and fragmented investigations to scientifically grounded models. Ultimately,

[40] https://doi.org/10.6028/NIST.SP.800-160v2r1

[41] https://csrc.nist.gov/glossary/term/cybersecurity

[42] https://www.cisa.gov/sites/default/files/2023-01/ppd-21-critical-infrastructure-and-resilience-508_0.pdf

[43] https://www.cisa.gov/sites/default/files/2023-01/StrategicPlan_20220912-V2_508c.pdf

[44] https://doi.org/10.6028/NIST.SP.800-160v2r1

[45] https://www.mitre.org/sites/default/files/2021-11/prs-15-1334-cyber-resiliency-engineering-aid-framework-update.pdf

[46] https://www3.weforum.org/docs/WEF_Cyber_Resilience_Index_2022.pdf

[47] https://www.ecb.europa.eu/paym/pol/shared/pdf/CPMI_IOSCO_Guidance_on_cyber_resilience_for_FMIs.pdf

models should enable impact evaluation to explore how events, actions, and response mechanisms affect cyber resilience.

Significant advancements in measurement are required to understand resilience properties of cyber systems and to evaluate strategies to mitigate and recover from disruptions. Improving cyber resilience will require the creation and use of effective metrics and indicators for assessing the design, implementation, and the use of resilience methods, across technological, human, and organizational perspectives.

Research Actions: Advance Science of Cyber Resilience

- Identify fundamental properties of cyber resilience and ways to specify cyber resilience requirements.
- Characterize the interactions of components, sub-systems, technologies, and processes that affect cyber resilience, including behavioral and economic aspects.
- Develop models and simulation capabilities that enable impact evaluation of how vulnerabilities, events, actions, and response mechanisms affect cyber resilience.
- Develop consistent and sound measures, statistically valid indicators, and efficient analytical methods to measure and assess cyber resilience across a variety of perspectives, such as system performance, risk to a mission, cost and benefit, and effectiveness.
- Develop techniques and measures to assess how system design and architecture contribute to and satisfy cyber resilience requirements.
- Develop secure cyber-resilient engineering techniques and training to improve standards for system design and the inclusion of cyber resilience in engineering tradeoffs.
- Develop approaches and techniques to integrate formal verification of functional and cyber resilience properties.
- Investigate the applicability of non-engineering disciplines such as ecology, medicine, and epidemiology for improving cyber resilience. For example, the effects of biological diversity on ecosystem resilience have motivated interest in artificial cyber diversity.

4.3.2 Research Objective: Improve Cyber Resilience by Design

Cyber resilience is achieved through both design and operation. Systems and system components must be designed and implemented to be resilient to attacks and the capabilities to defend, adapt, and recover must be available to provide resilience during the operation of the systems. From an engineering perspective, cyber resilience is a quality property of an engineered system, where an “engineered system” can be a system element made up of constituent components, a system, or a system-of-systems. Cyber-resilient systems are systems that have cybersecurity measures or safeguards “built in” as a foundational part of the architecture and design and display a high level of resiliency. Thus, cyber-resilient systems can withstand or seamlessly adapt to cyberattacks, faults, and failures and continue to operate at an appropriate level to carry out the mission-critical functions of the organization.

Cyber resilience is achieved through the application of the principles of trustworthy secure design[48] as part of a lifecycle-based, scientific, and engineering process. The design approach for engineering trustworthy and secure systems and achieving cyber resilience is intended to establish and maintain the

[48] https://doi.org/10.6028/NIST.SP.800-160v1r1

ability to deliver system capabilities at an acceptable level of performance while minimizing the occurrence and extent of loss. The system design must provide the intended behaviors and outcomes, avoid unintended behaviors and outcomes, prevent loss, and limit loss when it occurs. Using assurance-focused engineering practices, programming languages, and tools, developers are increasingly able to develop a system while simultaneously generating the assurance artifacts necessary to attest to the level of confidence in the system's capabilities to withstand attacks.

NIST Special Publication 800-160, Volume 2, *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*,[49] describes an engineering framework for understanding and applying cyber resilience by design, cyber resilience constructs that are part of the framework, a concept of use for the framework, and engineering considerations for implementing cyber resilience in the system life cycle. The engineering framework is employed in conjunction with NIST Special Publication 800-160, Volume 1, *Engineering Trustworthy Secure Systems*.[50]

The application of the cyber resilience engineering practices in system life cycle processes ensures that cyber resilience solutions are driven by stakeholder requirements and protection needs, which, in turn, guide and inform the development of system requirements for the system of interest. Such solutions need to be composed of combinations of technologies, architectural decisions, systems engineering processes, and operational policies, processes, procedures, or practices that solve problems in the cyber resilience domain. Cyber resilience solutions must provide a sufficient level of cyber resilience to meet stakeholder needs and reduce risks to organizational missions or business capabilities in the presence of a variety of threat sources, including the advanced persistent threat.

A significant challenge for cyber-resilient design and engineering is how to recognize explicitly that many new complex systems will be evolving, and the functional, security, and trust requirements and the emergent behaviors will be in a long-term feedback loop. The design and engineering process must proactively probe and account for the emergent behaviors for both positive and negative behaviors that are allowed, given the assumptions and constraints on the systems. Furthermore, the interactions of users with the environment and the complex systems will also be evolving and dynamic.

Research Actions: Improve Cyber Resilience by Design

- Identify secure software design principles that could eliminate large portions of common software weaknesses. For example, model-based designs can enable secure-by-design software, validate software execution against secure design principles, and be used to generate software to execute the intended functionality of a cyber-resilient system.
- Develop methods and tools that can reveal chains of emergent behavior at the architectural level in complex systems, as well as due to the interaction of the system with users and its environment.
- Research the composability properties of architecturally implied emergent behaviors of complex systems resulting in the use of the system in ways that are not intended. This includes the consequences and implications of incomplete, wrong, and likely unwritten assumptions and constraints.

[49] https://doi.org/10.6028/NIST.SP.800-160v2r1
[50] https://doi.org/10.6028/NIST.SP.800-160v1r1

- Develop methods and tools to assess the trade-offs between reliability and resilience, latency, and performance within complex systems. Given cyber resiliency goals, determine rigorous and mathematically optimized levels of latency and throughput for various operational scenarios.
- Develop methods and tools fully integrated into the development and maintenance processes to enable higher levels of availability, continuity, integrity, trustworthiness, and resilience of complex systems based on established rigorous and demonstrably causal metrics.
- Research and develop methodologies to allow concurrent holistic (top-down) and reductionist (bottom-up) development simultaneously while tracking security, safety, and other system-wide critical function requirements.
- Establish assessment methods for fully distributed systems that will trade maximum performance for/with maximum resilience in terms of the percentage of nodes or entities in the system that can be untrusted without impacting normal operations.
- Investigate how to improve cyber resilience by utilizing distributed ledger technologies that can be used to capture the state of a system (such as the history of the command-and-control communications and individual node information) in an efficient manner.
- Develop analytic tools and capability to model and assess the impact of social behavior on the system infrastructure to include the extent to which such behavior can invalidate the assumptions and security design such as the rise of influencers on the resilience of the network architecture.
- Develop practical in-situ test and evaluation capabilities for post-mission/event analysis for probabilistic systems where test scenarios and results are not directly repeatable.
- Research and develop practical and scalable multi-party computation schemes that could enhance any system role and improve cyber resilience. For example, for fully distributed key management or public key certificate authority in the presence of untrusted participating nodes.

4.3.3 Research Objective: Improve Cyber Resilience During Operation

Information systems should be assumed to be vulnerable to malicious cyber activities and security should be viewed as an ongoing process of self-evaluation and informed actions of adjusting and responding to threats as they evolve. The cybersecurity capabilities of Deter, Protect, Detect, and Respond[51] address the full range of operational cyber resilience goals, and by doing so, provide a structure for coordinating research and focusing on shared goals. The following objectives and research actions continue to be critical to improving cybersecurity broadly and are carried forward from the 2019 *Federal Cybersecurity R&D Strategic Plan*.

4.3.3.1 Deter

An effective way to secure a system from cyber threats is by deterring malicious cyber activities before they can compromise the system or the enterprise. Deterrence, in the broad sense used by this Plan, requires increasing the level of effort that adversaries must apply to achieve their objectives and increasing the possible negative consequences for adversaries from their actions. If adversaries judge that the likely costs of malicious activities, including risks of prosecution or sanctions, are greater than

[51] These four elements are similar but not identical to the five core functions in the NIST Cybersecurity Framework (https://www.nist.gov/cyberframework). This Plan is intended to guide cybersecurity R&D and is therefore broader in scope, while the five NIST core functions are focused on operational cybersecurity risk management. The differences between the NIST functions and this Plan's elements do not introduce any incompatibility between these efforts.

their expected benefits, they are more likely to be deterred from attempting the activities. Increasing both the required level of effort and the negative consequences for adversaries are needed for successful deterrence.

Research Actions: Deter

- Develop models of attackers, defenders, and users to assess attackers' risks, costs, and capabilities. Key factors to model are attacker effort (i.e., money, time, or computational cost), effectiveness, and risks, given the characteristics and capabilities of the defenders and users.
- Develop models to assess how cyber resilience readiness and capabilities improve deterrence, including how the knowledge and indicators that an organization is prepared to quickly overcome, respond to, and recover from a cyber instability deters adversaries.
- Develop capabilities to provide effective attribution of malicious cyber activities to their sources.
- Develop investigative and forensic tools for law enforcement to be able to successfully detect and prosecute cybercrime, domestically or across international jurisdictions.

4.3.3.2 Protect

Protection capabilities focus on creating components and systems that are resistant to attacks. Achieving resistance to attacks requires both limiting vulnerabilities in the first place and enforcing security policies and properties during operation.

Research Actions: Protect

- Effective authentication of users, devices, processes, and systems is needed to enable enforcement of security policies.
- Innovative access controls that utilize effective authentication are needed to support the implementation of security policies and authorizations. Advancement of efficient and correct implementation of cryptographic access control mechanisms (e.g., attribute-based encryption) is needed for untrusted environments (e.g., public cloud, IoT-edge environments).
- Advancements in cryptographic methods are needed to protect data from unauthorized disclosure, to support authentication and access control, operate directly on encrypted data, and to operate in constrained environments.
- Implementation errors can undermine the security of well-designed components. To reduce product vulnerabilities, tools and practices for software and hardware development (e.g., correctness-by-construction) are needed that significantly improve developer productivity and operational system performance.
- Design flaws may creep in during system development. In addition to undergoing functional testing, components and systems should be subjected to rigorous security analysis throughout the development process. Improvements in analysis methods and tools are needed to continue to identify and eliminate vulnerabilities and design flaws before a product goes to market.
- Given the continuing prevalence of memory safety vulnerabilities, identify effective approaches to accelerate maturity, adoption, and security of memory safe programming languages. Advance both software- and hardware-based solutions to mitigate and eliminate memory safety vulnerabilities.
- When defects are identified during operation, the deployed systems must be updated. Secure mechanisms for updating software or firmware are needed to secure products throughout their

lifecycles. Securing the software and hardware supply chain is also a critical protection capability. See Section 5.1 for further details and research actions in this area.

4.3.3.3 Detect

Detection seeks to ensure that system and network owners and users have situational awareness and understanding of ongoing (authorized and malicious) activities and can move toward largely automated warning and response abilities.

Research Actions: Detect

- To defend networks and systems, it is necessary to identify all of a system's critical assets, track when devices have been added or removed, and monitor attributes and anomalies associated with the users. Real-time change detection is essential, including schemes that are flexible for dynamic network conditions and enable comparisons against known good system states.
- Changes in system configuration, installation of new applications, or discovery of new techniques may reduce a system's level of protection or create new vulnerabilities. Tools are required to identify shortcomings in protection measures in real time so the situation can be remediated.
- Advances are required to ensure that detection techniques can reliably detect the full range of adversaries' malicious cyber activities and reduce detection time.
- Methods and tools are needed that can detect zero-day malware and innovative sequences of operations with acceptable levels of false positives and negatives.
- Scalable mathematical techniques capable of extracting useful information from extremely large system and network log datasets are needed to enable more effective and rapid detection of malicious cyber activities.

4.3.3.4 Respond

Effective cyber resilience requires the ability to adapt, counter, recover, and adjust to malicious, faulty, and erroneous cyber activities and events. Systems must withstand such events to ensure that their critical mission and operational functions still meet minimum performance requirements and substantial damage is avoided. Resilient systems will continue to perform correctly during and after such activities and will recover from adverse effects. To sustain resilience, systems must also dynamically adapt to changing threats and the socio-technical context of the digital environments. Moreover, effective response includes exposing, limiting, disrupting, or blocking malicious activities.

Research Actions: Respond

- Advances are needed to measure key properties and attributes of system components and assess potential damage amidst evolving threat landscape and system requirements, thereby enabling response and recovery to a known good state.
- Develop methods to adjust to actual, emerging, and anticipated disruptions so that essential mission and organizational needs can continue to be met. Such methods should support the identification and understanding of risk dependencies and how response actions in one part of the system may affect other parts of the system.
- Detection of a cyberattack or system degradation may not always be possible, particularly when dealing with advanced cyber threats that can hide or remove evidence of activities. Advances in preemptive actions are needed that can maintain cyber security and resilience of a system without the need to identify an attack or degradation.

- Investigate approaches that effectively integrate human factors as a source of cyber resilience. In times of crisis, human traits such as creativity, flexibility, and improvisation can be the decisive factors in a successful mitigation and resolution of a cyberattack or incident. Investigate organizational factors that contribute to, as well as impede, cyber resilience.
- Provide methods to manage risks at multiple layers or scales (e.g., component, device, system, systems of systems, enterprise, or international coalition) and enable collective responses to a range of specific types of malicious cyber activities, such as distributed denial-of-service attacks or advanced persistent threats.

5 Federal Priority Application Scenarios

Section 4 describes research objectives in three priority areas: Protect People and Society, Develop Means to Establish and Manage Trust, and Strengthen Cyber Resilience. The priority areas illuminate fundamental and translational challenges in cybersecurity but also opportunities for substantial progress in securing the digital ecosystem. The priority areas are broad, interdisciplinary, and require innovations and contributions from a number of sciences and technologies.

While broad advancements in cybersecurity are necessary, the federal government, through executive and legislative actions, has also identified specific topics and domains that have strategic importance to the nation. This section provides recommendations for research in several application scenarios that are significantly called out for action by the Administration and Congress. The application scenarios here are drawn from: *EO-14028: Improving the Nation's Cybersecurity*, 2023 *National Cybersecurity Strategy*, *Blueprint for an AI Bill of Rights*, *OMB-OSTP R&D Priorities, CHIPS and Science Act of 2022*, and *Inflation Reduction Act of 2022*.

5.1 Protect Software and Hardware Supply Chain

In an increasingly interconnected digital society, the nation's critical infrastructure systems will continue to rely on software and hardware developed and manufactured by domestic and foreign suppliers of varying levels of trust. This dependence on untrusted suppliers introduces multiple sources of systemic risk to our digital ecosystem. These risks include a lack of transparency into processes and components being incorporated into critical information and operational technologies; inability to immutably retain and attest to integrity of software and hardware during design and development; inability to independently verify the assurance properties of technologies during and after acquisition; and inability to effectively detect, respond, and recover from previously unidentified supply chain issues during the operational life cycle phase at speed and scale.

These risks are further exacerbated by the geospatial dispersion and heterogeneity inherent in the digital ecosystem, both from a developer/supplier perspective and from an end-user/maintainer perspective. The rapid pace of technological advance and the diversity of where and how these technologies are employed to support critical functions make it increasingly difficult to establish secure, trustworthy, and resilient supply chains. Identifying and mitigating the potential risks and vulnerabilities that can be inserted throughout a technology's lifecycle, in addition to the emergent risks that can arise from the integration of multiple technologies into systems of systems, is becoming an intractable problem.

This section highlights research objectives and actions related to securing software and hardware supply chains as part of an overall goal to increase cyber resilience through a focus on security by design.

5.1.1 Research Objective: Increase Ability to Attest to Supply Chain Integrity Through Design and Development

Research Actions: Increase Ability to Attest to Supply Chain Integrity Through Design and Development

- Develop approaches to expand critical supply chain information visibility while preserving privacy and confidentiality of sensitive information. Supply chain participants need to retain control of proprietary information to enable free market competition; however, some essential elements of the supply chain need to be examined in aggregate to ensure the entire supply chain can achieve availability objectives.

- Develop methods for secure and trustworthy processes and components to protect the design and development toolchain.
- Develop effective modeling and simulation approaches and engineering techniques that can stress test the cyber resilience and trustworthiness of the supply chain and enable analysis of causal metrics across multiple independent parties while preserving confidentiality of sensitive information.
- Develop methods to enhance supply chain traceability and resiliency through techniques that reliably predict, detect, and verify the presence of naturally occurring and immutable properties of supply chain components throughout fabrication and integration.
- Develop techniques to identify counterfeit components at scale. Current techniques are resource intensive, inefficient, and can only be done on an individual or small scale. Advances are required to enable more effective and efficient inspections to identify counterfeits within large quantities of systems in a timely manner.
- Research techniques to quantify and increase the reliability of AI-assisted design and development tools.
- Develop capabilities to enhance the design and development of code. This includes tools for developing in, and/or converting, existing software to memory-safe programming languages. Develop hardware-layer technologies that can mitigate memory safety vulnerabilities.
- Develop effective and efficient techniques to establish, validate, and verify chain-of-trust across the supply chain.

5.1.2 Research Objective: Increase Ability to Verify and Maintain Ongoing Supply Chain Integrity Throughout Operations

Research Actions: Increase Ability to Verify and Maintain Ongoing Supply Chain Integrity Throughout Operations

- Develop capabilities to enhance the ability to federate and analyze cybersecurity threat information and develop mitigations at scale while preserving the privacy and confidentiality of sensitive information. Enable predictive and indicator analysis for runtime protection across networks.
- Develop methods and tools to apply a fully distributed platform agnostic distributed ledger technology to enhance cyber resilience of supply chains through the collection and sharing of public source information across supply chain partners without requiring the explicit sharing of potentially sensitive data.
- Develop approaches to integrate the provenance information of hardware, software, and data to provide greater insight into emergent or latent systemic supply chain risks and evolving threat vectors and enable more comprehensive risk management and incident response. Increase ability to independently generate extended bills of materials, exchange vulnerability and exploitability information, and verify ongoing behavioral consistency.
- Develop techniques to enhance provenance information and visibility across supply chains through distributed ledger technology-based approaches enabling rapid, effective, and tailored cyber incident response. Develop tools and techniques to utilize provenance information to enable tailored incident response.

- Develop approaches to enhance the diagnostics and continuous integrity scanning/verification process (e.g., periodic testing and integrity proofing).
- Develop secure methods for updating software or firmware to secure products throughout their lifecycle.
- Develop approaches for real-time change detection including schemes that are flexible for dynamic network conditions and enable comparisons against known good system states.

5.2 Realize Secure and Trustworthy AI

Advancing safe, secure, and trustworthy AI that protects people's rights and safety and harnessing it to accelerate the nation's progress is a strategic priority for the Biden-Harris Administration. President Biden has taken a number of actions to address this priority, including signing the *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*.[52] Among its directives, the Executive Order instructs federal agencies to establish standards for AI safety and security, protect Americans' privacy, advance equity and civil rights, stand up for consumers and workers, promote innovation and competition, and advance American leadership in AI abroad.

This section considers the trustworthiness of AI systems. Cyber security and cyber resilience is a critical part of these systems' trustworthiness, though trustworthy AI also depends on other factors. NIST[53] has identified seven attributes necessary for trustworthy AI: Validity and Reliability; Safety; Security and Resiliency; Accountability and Transparency; Explainability and Interpretability; Privacy; and Fairness with Mitigation of Harmful Bias.

Many of these attributes, and the associated technical challenges and relevant R&D, are considered in other examinations of AI. For example, Strategy 3 in the *National AI R&D Strategic Plan 2023 Update*[54] focuses on the attributes of accountability, explainability, privacy, and fairness.

Within the broader definition of Trustworthy AI, and expanding on key concepts from the *National AI R&D Strategic Plan 2023 Update*, this Plan focuses more specifically on the R&D needed to realize AI that is safe, secure, and resilient.

Advances in AI are breathtaking, with exciting new capabilities spanning natural language processing, image recognition, data analytics, autonomous systems, and content generation. Unfortunately, just as the networks and computing systems that enable such capabilities have proven to be difficult to secure and assure, so too is machine learning-based AI. ML-based AI systems can be manipulated, evaded, and misled, creating significant security issues for applications that utilize them.[55] The spectrum of attacks on AI and ML is evolving and covers all phases of the ML lifecycle—from design, development, to training, testing, and operation. Over a dozen classes of attacks on ML have been identified.[56] Modern machine learning expands the attack surface for cyber adversaries, and this consequence has spawned a field of

[52] https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/

[53] https://www.nist.gov/trustworthy-and-responsible-ai

[54] https://www.whitehouse.gov/wp-content/uploads/2023/05/National-Artificial-Intelligence-Research-and-Development-Strategic-Plan-2023-Update.pdf

[55] https://par.nsf.gov/servlets/purl/10173547

[56] https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-2e2023.ipd.pdf

study termed "adversarial machine learning (AML)."[57] AML research is needed to address the potential for adversarial manipulation of training data, adversarial exploitation of model vulnerabilities, and unauthorized disclosure of sensitive information represented in the data or about the model itself. Of particular concern are cybersecurity challenges associated with foundation models that include large language models (LLMs) and generative AI (GAI).

As the use of LLMs and other GAI becomes commonplace, the cybersecurity risks from such modern AI technologies can span organizations and have societal impacts. Recognizing these risks, the Biden-Harris Administration has issued a *Blueprint for an AI Bill of Rights* seeking to prevent the use of technology, data, and automated systems in ways that threaten the rights of the American public. Managing the risks posed by AI is an Administration priority.[58] In particular, NIST has released the *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*,[59] a guide and a resource to the organizations and individuals designing, developing, deploying, or using AI systems to help manage the many risks of AI and promote trustworthy and responsible development and use of AI systems.

The major challenges that the cybersecurity community can help address are:

- Assure the security of AI
- Engineer verifiable and resilient AI systems
- Enable trusted collaboration between humans and AI

5.2.1 Research Objective: Establish Formal Assurance Methods for AI

LLMs and GAI systems demonstrate impressive competence at dialog, question answering, and content generation. However, at the same time, LLMs can sometimes generate inaccurate results in ways that are untrustworthy, harmful, or aberrant. Overall, ML-based AI's vulnerabilities and cybersecurity risks are poorly understood, and it seems likely that new vulnerabilities will be discovered. It is essential to understand and quantify the cybersecurity risks of ML and GAIs in order so that principled assessments of their fitness can be made before they are used in mission applications.

One of the more difficult challenges with AI is evaluation and assurance, since AI-based systems tend to resist traditional approaches to testing, verification, inspection, and analysis. It is not possible to fully test an AI-based system for every situation it will ever encounter, so new techniques are needed for testing, verifying, and validating AI-based systems. As noted by NIST,[60] a further fundamental challenge in securing AI systems is the lack of information-theoretically secure ML algorithms. Consequently, securing ML systems today is an ad hoc and fallible process. Applying formal methods to machine learning can provide much-needed correctness and security guarantees. As a growing field, the application of formal methods for securing and verifying AI would benefit from increased support.

Research Actions: Establish Formal Assurance Methods for AI

[57] https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-2e2023.ipd.pdf

[58] https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/21/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-leading-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/

[59] https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf

[60] https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-2e2023.ipd.pdf

- Develop approaches for quantifying the security risks posed by frontier AI (e.g., LLMs, GAI, data-intensive AI, and other advanced AI models) considering the full AI pipeline.
- Develop a standardized AI cybersecurity assessment methodology for frontier AI, which can be governed by a common standard for compliance.
- Develop approaches to apply formal methods to machine learning algorithms, with the ability to scale them effectively to the large ML models used today.
- Create secure and high assurance software and systems engineering methodologies, techniques, tools, and practices to facilitate the development of AI-based systems that are secure and trustworthy.

5.2.2 Research Objective: Engineer Verifiable and Resilient AI Systems

AI technology presents a dramatic enlargement of the attack surface for systems with which they interact and/or are integrated, and so have the potential to exacerbate or enable a range of vulnerabilities.[61] In general, AI systems are designed to operate in complex environments and within specific contexts, with a large number of potential states that cannot be exhaustively examined or tested. A system may confront conditions that were never considered during its design when used in novel contexts. Current methods for development of such systems remain primarily based on trial-and-error, with limited interpretability of or insight regarding these systems' internal function. These developments can be costly, risky, and demanding of very high levels of expertise.

Before AI can be used in critical systems it must be secure against a wide range of cyberattacks. Improved techniques are needed for defending against deception and other adversarial attacks on AI systems. Deception attacks, whereby an adversary inputs data engineered to cause erroneous results, can enable adversaries to take control of autonomous systems, alter conclusions of decision support applications, and compromise tools and systems that rely on machine learning and AI technologies. Current techniques for defending AI have proven brittle due to a focus on individual attack methods, weak methods for testing and evaluation, and an inability to understand human alignment. Techniques are needed to address the current limitations of defenses and produce AI systems suitable for use in adversarial environments. Theory regarding potential fundamental limits on achievable AI robustness is also needed.

Datasets used to train AI systems may become detached from their original and intended context or may become stale or outdated relative to deployment context. Intentional (including adversarial) or unintentional changes to training data may fundamentally alter trustworthiness and performance of AI systems. LLMs can also create privacy and legal concerns because private and confidential data that may have been used to train a model can be revealed in inference attacks.[62]

Research Actions: Engineer Verifiable and Resilient AI Systems

- Develop techniques for threat modeling, testing, evaluation, verification, and validation of systems that incorporate multiple AI-enabled components with regards to their security, resilience, and trust properties.
- Develop new abstractions, architectures, assurance techniques, and testing processes that can facilitate the analysis and synthesis of complex systems that include AI-based components.

[61] https://airc.nist.gov/home
[62] https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-2e2023.ipd.pdf

- Develop techniques for detecting and preventing compromise and ensuring the integrity of machine learning applications. Develop enhancements that enable resilience to adversarial attacks.
- Create techniques to prevent reverse engineering of source training data and data leakage by machine learning systems.
- Develop federated approaches for secure and privacy-preserving distributed, federated or collaborative machine learning across multiple data sources, entities, and institutions. Such approaches should address end-to-end security and trust, and consider issues such as verifiably secure composability and interoperability.

5.2.3 Research Objective: Improve Trusted Collaboration between Humans and AI

The performance of an AI system is often substantially affected by human interactions and, in some cases, variation in human responses may affect the safety of the system. Systems that depend on the implicit trust of the user, such as autonomous vehicles, must be transparent (i.e., the system operates in a manner that is fully visible to the user), credible (i.e., the system's outputs are accepted as sensible by the user), auditable (i.e., the system can be evaluated to high degrees of technical detail), reliable (i.e., the system acts as the user intended), and recoverable (i.e., the user can recover control when desired). Establishing such trust is a significant challenge because the barriers to such trust arise from the intrinsic design and operation of today's ML systems.[63] For example, human-established trust is in part based on an expectation that the other party can conceptualize knowledge and behavior and successfully apply it in new circumstances. On the other hand, today's ML systems are unable to conceptualize and apply patterns the way humans can, a consequence of how today's ML systems function (i.e., by finding statistical associations and by making predictions through classification and regression).

New technologies and solutions are needed to enable AI systems to function not only as tools that facilitate human action but as trusted partners to human operators. Of particular interest are systems that can interpret human goals and constraints, and learn, reason, and apply knowledge gained through experience to respond safely and intelligently to new events. Designing systems with effective human and AI collaboration mechanisms is especially important in domains where the pace of operations exceeds that at which unaided humans can orient, understand, and act. For example, advances are needed to enable effective collaboration among autonomous agents and human cybersecurity professionals for effective cyber defense and to combat emerging threats from AI-driven attacks.

The issue of alignment, which involves understanding how well an AI system incorporates the intended goals, preferences, system's trust assumptions, or ethical principles of its human developers, has gained heightened attention with recent advancements of frontier AI. Due to the difficulty of translating human goals into computer instructions, the behaviors of an AI system may not match the goals that were intended by the developer and are desired by the user. As the lack of alignment becomes apparent, trust will likely be lost. AI alignment research has identified several principles (e.g., interpretability, controllability) as key objectives for AI alignment. Additional AI alignment research is required to enable

[63] https://media.defense.gov/2023/Sep/26/2003308982/-1/-1/0/TRUSTING%20AI_INTEGRATING%20ARTIFICIAL%20INTELLIGENCE%20INTO%20THE%20ARMY_S%20PROFESSIONAL%20EXPERT%20KNOWLEDGE.PDF

machine learning systems that are sufficiently trustworthy that they can be used in safety- and mission-critical applications.

Research Actions: Improve Trusted Collaboration between Humans and AI

- Develop principles, methods, technologies, and best practices for secure and trusted collaboration and interaction between humans and AI. New socio-technical approaches are needed to enable trusted human-AI teaming.
- Develop theories, models, and approaches to enable trusted human-AI collaboration by demonstrating the alignment of AI and machine learning systems with the intended goals, preferences, and ethical principles of its human developers and users.

5.3 Secure the Clean Energy Future

A clean energy revolution is taking place across America, underscored by the steady expansion of the U.S. renewable energy sector. Funding from the *Infrastructure Investment and Jobs Act of 2021*[64] and the *Inflation Reduction Act of 2022* has spurred a new industrial revolution building America's clean energy future. Additionally, the federal government and national defense priorities encourage transition to clean energy technologies such as zero-emission vehicles and energy efficient buildings that are powered by carbon pollution-free electricity. The 2020 *DOE Roadmap for Wind Cybersecurity*[65] identified the increasing utilization of sustainable energy and the necessity to identify vulnerabilities, raise awareness and formulate strategies for cybersecurity defense, response, and future protection.

The NCS identifies clean energy technologies as a critical R&D focus area for U.S. leadership in the coming decade. The NCS emphasizes the need to embrace security and resilience by design to secure the nation's clean energy future. DOE, as indicated in the NCS, will lead the government's effort to secure the clean energy grid of the future and will continue to promote cybersecurity in the energy sector in partnership with industry, States, federal regulators, Congress, and other agencies.

Research Actions: Secure the Clean Energy Future

- Incorporate cyber-resilient-by-design principles in clean energy technologies. For example, develop cyber secure energy storage solutions, distribution control systems, building management systems, and Electric Vehicle Supply Equipment (EVSE) that are inherently secure from or resilient to a cyber or cyber-physical threat.
- Develop cyber secure and resilient architectures for the communications infrastructure required to operate and manage clean energy systems.
- Develop approaches to effectively identify vulnerabilities in the combined cyber and physical energy systems and develop standards for the protection of sustainable energy infrastructures and information sharing among energy stakeholders.
- The clean energy future will include a variety of new stakeholders, such as aggregators and service providers. Research is needed to understand cybersecurity, trust, and privacy considerations for the new stakeholders, as their responsibilities evolve across the clean energy environment.

[64] https://www.congress.gov/117/plaws/publ58/PLAW-117publ58.pdf
[65] https://www.energy.gov/sites/default/files/2020/08/f77/wind-energy-cybersecurity-roadmap-2020v3.pdf

- Develop enhanced anomaly detection that will be effective in the distributed environments of clean energy systems. Develop new approaches that can leverage technologies such as machine learning to model and predict anomalies in such new environments.
- Develop modeling capabilities to understand systemic and localized cybersecurity impacts, especially those from bidirectional cyber threats, such as a Vehicle to Grid threat vector, or how distributed infrastructure such as smart buildings and EVSE may be maliciously leveraged to impact the electric grid.

6 Critical Dependencies

Advancements in this Plan's priority areas and application scenarios critically depend on continuing development in the following areas.

6.1 Advance Cybersecurity Metrics, Measurements, and Evaluation

The need for sound metrics, measurements, and evaluation methodologies pervades the entire field of cybersecurity. Many research objectives and actions discussed in previous sections depend on effective capabilities to measure and evaluate a broad spectrum of cybersecurity, resilience, and trustworthiness characteristics. This section brings the various cybersecurity measurement needs discussed in this Plan into one location, to raise the visibility and priority of this important area.

Cybersecurity is not a goal for its own sake but rather a reflection of the real-world needs of users, developers, and other stakeholders. As a result, the cybersecurity evaluation of a system should reflect and be informed by the needs of its stakeholders and its deployment environment: a system that is secure in one deployment environment might fail catastrophically or become inadequate in others. Conversely, a user's security requirements may be overly ambitious or unrealistic to the extent that they cannot be addressed by state-of-the-art security or privacy solutions. Presently, security and privacy technologies are often evaluated with limited consultation with users and stakeholders.

Furthermore, practitioners are faced with very practical questions, such as, how to evaluate the security of competing commercial products, and how to determine a potential cybersecurity risk of proposed technologies and services. Practitioners need answers to such questions today, even though research on these topics is ongoing. This Plan envisions productive interactions between those research activities and the dependencies discussed in this section: research will inform evaluations, and the success and failures of these evaluations will inform research.

Measurements and evaluation depend on the existence of metrics. Metrics help an organization understand, implement, and use a cybersecurity program to support its mission or business objectives. To achieve this goal, cybersecurity metrics R&D should focus on methodologically developing a technology-agnostic, tailorable, risk-based information security metrics program for all levels of an organization, including the organization's component products, services, and supply chains.

Currently, many metrics are in use by organizations. However, many of these metrics are: (a) insufficient to the point that they are not useful for making organizational decisions, (b) often not reusable by other organizations, and (c) difficult to meaningfully compose in complex environments.

Enterprise and consumer users as well as technology developers are often interested in predicting high-level properties of technologies, such as dependability, safety, and security, which can be difficult to measure. In contrast, most properties that can be measured are often not directly related to the desired high-level properties. Clearly differentiating the high-level properties from the measurable quantities is necessary for creating a more solid foundation for cybersecurity metrology, that will in turn increase software assurance.[66]

Understanding opportunities to capture practitioners' activities and translating these activities into assurance metrics are needed. An exemplar of this activity is to understand how combinations of tools,

[66] https://doi.org/10.6028/NIST.IR.8101

practices, and programs can support metrics programs, such as code quality, which will provide insights into metrics and complement assurance claims to support security from components to systems and across lifecycles.

Research Actions: Advance Cybersecurity Metrics, Measurements, and Evaluation

- Expand and refine quantifiable concepts for cybersecurity measurements. Advance general metrology issues such as dimensional analysis with counted quantities, generalized models of uncertainty, and characterization of complex systems for cybersecurity.
- Strengthen the foundations of cybersecurity metrics by developing capabilities to prevent comparing and combining disparate measures (which leads to problems with the validity of results), and to minimize subjectivity (which can distort the measurements).
- Develop methods and tools to validate cybersecurity metrics to establish their utility in different contexts and to support their use in assessments of technologies.
- Study how methodologies of evaluation and measurements can be used to improve cybersecurity solutions. For example, develop effective techniques to capture feedback from users and stakeholders after a technology was developed and fielded, to generate new concepts for cybersecurity innovation.
- Formulate a means to objectively measure and evaluate the effectiveness of cybersecurity solutions, ranging from commercial products to R&D efforts, with respect to users' needs or requirements.
- Develop cybersecurity evaluation models that can account for technology, socioeconomics, and policy factors. Such models should be testable, reproducible, and subject to the evaluation of their effectiveness.

6.2 Cybersecurity Research, Development, and Experimentation Infrastructure

Effective cybersecurity research, development, and experimentation requires access to infrastructure that is up to date and has commensurate capabilities to support innovation at the scope and scale needed to pace both the domain's evolution and adversaries' own advancements. However, access to such advanced cybersecurity research and experimentation infrastructure continues to be a hurdle for researchers.

The current state of cybersecurity research, development, and experimentation infrastructure is characterized by disjoint research platforms, discrete funding and developmental resources, and a lack of overall orchestration of resources and long-term governance. The national cyber landscape once again finds itself challenged—this time by the emanation of third-wave AI technologies. Rather than relying on an ensemble of disparate endeavors to confront this challenge, the federal government should instead recognize the potential inflection point in its cyber research infrastructure strategy and work towards a whole-of-nation response founded upon public-private partnership. Such public-private partnership should aim to establish robust, federated cybersecurity research, development, and experimentation infrastructure, including testbeds, test-ranges, appropriate data, and critical infrastructure simulation capabilities that would enable multidisciplinary research spanning the cyber, physical, and cognitive domains with support for live and virtual experimentation.

7 Implementing the Strategy

This section identifies the roles for the federal government, academia and research organizations, and the commercial sector, and identifies strategies for ensuring coordination of cybersecurity R&D within and across these sectors.

Federal Research Agencies

The coordinated R&D activities of this Plan are facilitated or carried out by federal agencies and departments with varying missions but complementary roles. This arrangement ensures that the full spectrum of R&D approaches is represented and engaged. Each agency or department is encouraged to incorporate these research priorities into its research plans and programs, drawing on its individual strengths and in the context of its mission. It is expected that agencies will detail their approaches for implementing this Plan in their strategies, implementation plans, or roadmaps.

Science agencies, such as the National Science Foundation, should solicit and fund multidisciplinary research and continue to demand strong scientific methods in all funded initiatives. Mission agencies, such as the Department of Homeland Security, primarily fund applied research with a near-term or mid-term horizon to meet immediate and future mission requirements. Mission-specific R&D is often incremental in nature, and agencies should make efforts to ensure that the desired functionality is not already available from the private sector or other federal agencies. Both science and mission agencies should pursue near-term R&D if it is directly related to mission-specific needs or creates public goods that industry is not incentivized to pursue.

Research-funding agencies also have obligations to ensure that their R&D investments reduce inequities and create opportunities for all in ways that strengthen the values of the nation, equip under-resourced educational institutions and underserved communities to successfully participate in R&D activities, cultivate equitable Science, Technology, Engineering, and Math (STEM) education and cybersecurity workforce ecosystem, and ensure free, immediate, and equitable access to federally funded research results and data, consistent with the Administration's FY 2024[67] and FY 2025[68] *Research and Development Budget Priorities*, and *Ensuring Free, Immediate, and Equitable Access to Federally Funded Research*[69] memoranda.

Academic and Research Organizations

The research community is critical in effectively addressing the research priorities in this Plan. Researchers in academia are encouraged to consider both disciplinary and interdisciplinary approaches, measurable efficacy and efficiency, reproducibility of experiments, and strategies for transitioning successful research into practice when developing proposals and initiating research in this area. Where possible, researchers should provide comparisons against open datasets to enable comparison and evaluation of competing techniques. Use of open datasets also enables reproducibility of experiments, which is a basic scientific tenet. Academic institutions are strongly encouraged to value multidisciplinary cybersecurity research, even where publication occurs in nontraditional journals for the field. Institutions are also encouraged to value research with rigorously defined models and experimental design.

[67] https://www.whitehouse.gov/wp-content/uploads/2022/07/M-22-15.pdf
[68] https://www.whitehouse.gov/wp-content/uploads/2023/08/M-23-20.pdf
[69] https://www.whitehouse.gov/wp-content/uploads/2022/08/08-2022-OSTP-Public-access-Memo.pdf

Research organizations and professional societies are natural partners in cybersecurity R&D efforts, by producing research strategies, organizing conferences, and publishing journals. By establishing publication requirements for documented efficacy and efficiency, these organizations can greatly aid and improve scientific rigor in the cybersecurity field.

Commercial Sector

Private sector R&D is typically internal and focused on product development goals based on the specific needs of the company as well as on profitability and turnaround time. Budgets for commercially funded cybersecurity research are usually comparatively modest for even the largest IT companies. Nonetheless, there are opportunities for the R&D activities of the private sector and the public sector to be synergistic and complementary. This Plan outlines a number of areas and topics for engagement with the commercial sector; additional opportunities include enabling access to real-world data needed in cybersecurity research, defining common use cases for research purposes, and for commercial entities to jointly identify precompetitive research areas in which public-private partnership funding would be most productive.

Coordination and Collaboration

This Plan calls for increased coordination and collaboration across all sectors, and with international partners, to make measurable and effective progress in cyber security and resilience and to avoid redundant research initiatives. The federal cybersecurity R&D community engages with industry via many public-private partnerships, which need to continue to be enhanced and strengthened.

The partnerships include industry advisory boards, programs that engage innovators, such as the DOD National Security Innovation Network and the DHS Silicon Valley Innovation Program, and centers where industry and government can collaborate such as the NSA Cybersecurity Collaboration Center and the NIST National Cybersecurity Federally Funded Research and Development Center (FFRDC). In addition, the National Cybersecurity Center of Excellence is an example of a federal, state, and local government partnership (NIST, the State of Maryland, and Montgomery County, MD), which focuses on accelerating the adoption of secure technologies. Multisector efforts focused on specific technology domains should be further expanded, such as the National Artificial Intelligence Research Institutes led by NSF in partnership with NIST, DOD Office of the Under Secretary of Defense for Research and Engineering, and several corporations and foundations.

Research coordination between federal departments and agencies is facilitated by the National Science and Technology Council. Unclassified federal R&D efforts in networking and information technology are coordinated by the NITRD Subcommittee and its National Coordination Office. Classified research efforts are coordinated by the NSTC Special Cybersecurity Operations Research and Engineering Subcommittee.

Each year, the NITRD Program compiles and produces a Supplement to the President's Budget Request that provides highlights of agency R&D activities in various areas of information technology and networking. In the Supplement, the section describing NITRD’s Cyber Security and Information Assurance Interagency Working Group provides an overview of planned federal investments in unclassified cybersecurity R&D. The annual *Federal Cybersecurity R&D Strategic Plan Implementation Roadmap* (an online appendix to the Supplement, available at https://www.nitrd.gov/publications/), provides information about the activities the agencies are pursuing in implementing this Plan.

8 Acronyms

AFRL	Air Force Research Lab
AI	Artificial Intelligence
CHIPS	Creating Helpful Incentives to Produce Semiconductors
DARPA	Defense Advanced Research Projects Agency
DHS	Department of Homeland Security
DOD	Department of Defense
DOE	Department of Energy
ENISA	European Union Agency for Cybersecurity
EVSE	Electric Vehicle Supply Equipment
FAA	Federal Aviation Administration
FFRDC	Federally Funded Research and Development Center
FY	Fiscal Year
GAI	Generative Artificial Intelligence
IIRD	Information Integrity R&D
IoT	Internet of Things
IT	Information Technology
LLM	Large Language Model
MD	Maryland
ML	Machine Learning
NCO	National Coordination Office
NCRI	National Cyber Research Infrastructure
NCS	National Cybersecurity Strategy (2023)
NCWES	National Cyber Workforce and Education Strategy
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
NITRD	Networking and Information Technology Research and Development
NRL	Naval Research Laboratory
NSA	National Security Agency
NSF	National Science Foundation
NSTC	National Science and Technology Council
OMB	Office of Management and Budget
OSTP	Office of Science and Technology Policy
OT	Operational Technology
OUSD R&E	Office of the Under Secretary of Defense for Research and Engineering
R&D	Research and Development
STEM	Science, Technology, Engineering, and Math