2021 Cybersecurity and Privacy Annual Report

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST SPECIAL PUBLICATION 800-220

Fiscal Year 2021
Cybersecurity & Privacy Annual Report

PATRICK O'REILLY, EDITOR
Computer Security Division
Information Technology Laboratory

KRISTINA RIGOPOULOS, EDITOR
Applied Cybersecurity Division
Information Technology Laboratory

CO-EDITORS:
Larry Feldman
Greg Witte
Huntington Ingalls Industries
Annapolis Junction, Maryland

THIS PUBLICATION IS AVAILABLE FREE OF CHARGE FROM
https://doi.org/10.6028/NIST.SP.800-220

SEPTEMBER 2022

U.S. DEPARTMENT OF COMMERCE
Gina M. Raimondo, Secretary

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Laurie Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

Table of Contents

Foreword 1

Focus Area 1: Cryptographic Standards and Validation 2

Focus Area 2: Cybersecurity Measurement 6

Focus Area 3: Education and Workforce 9

Focus Area 4: Identity and Access Management 12

Focus Area 5: Privacy Engineering 15

Focus Area 6: Risk Management 18

Focus Area 7: Trustworthy Networks 25

Focus Area 8: Trustworthy Platforms 31

ITL Leadership and Participation in National and International Standards Programs 35

Opportunities to Engage with the NIST on Cybersecurity and Privacy 37

Foreword

Pablo Picasso famously said, “action is the foundational key to success". At the National Institute of Standards and Technology (NIST), we have been a part of the action in the cybersecurity world since the very beginning, and this year is a big one for us. We are celebrating a major milestone as we hit 50 years of cybersecurity at NIST. For 50 years, NIST—formerly the National Bureau of Standards (NBS), until 1988—has conducted research and developed guidance that has led to extraordinary advancements in cybersecurity.

We take pride in our rich history and work to honor the tradition of fostering an open, transparent, and collaborative environment where we cultivate trust in technology. Our dynamic projects are of global importance because they help advance technology, cybersecurity and privacy standards and guidelines, and measurement science for all of us. We value success, and all the learning and collaboration that comes along with it.

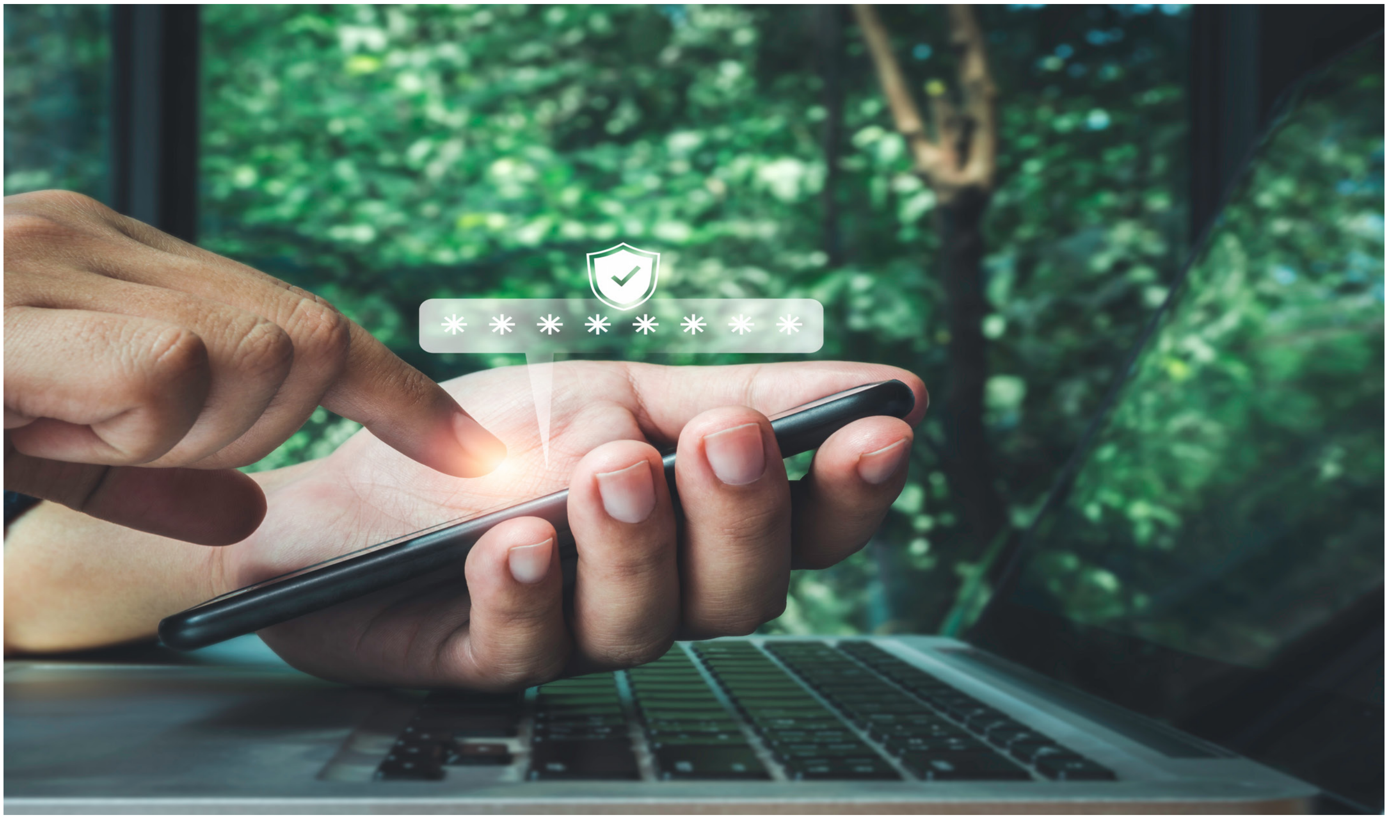
This annual report is organized into eight key areas: cryptographic standards and validation, cybersecurity measurement, education and workforce, identity and access management, privacy engineering, risk management, trustworthy networks, and trustworthy platforms. This past year, NIST conducted research and demonstrated practical applications in several key priority areas, including post quantum cryptography (PQC), cybersecurity in supply chains—which was included in an Executive Order from the President in 2021—zero trust, and control systems cybersecurity. We also initiated research in some new areas, including exploring the cybersecurity of genomics data.

We have a lot planned for 2022 as we help organizations better manage risk (for example, we are launching an update process for the Cybersecurity Framework and reviewing a host of other NIST frameworks and guidance documents with an eye on improving their alignment). We have also made selections of finalists and alternate candidates to be considered for PQC standardization. Stay tuned for updates to our foundational digital identity guidelines and for information on some of our new projects related to cybersecurity workforce and privacy (and be on the lookout for a Workforce Framework). We also will unveil a new tool that will make it simpler and quicker for users of NIST cybersecurity and privacy products to navigate content across NIST resources.

While Picasso was famous for a completely different form of art, cybersecurity and privacy is our ‘art’—and our science—and we are ready for 50 more years of innovation, collaboration, and action.

Kevin Stine
NIST Chief Cybersecurity Advisor

1 | Cryptographic Standards and Validation



Credit: Shutterstock

Cryptographic standards, algorithms, and methods for encryption, key-establishment, and digital signatures provide a critical foundation for cybersecurity. NIST cryptographic standards have been adopted as essential tools to secure communications and protect computing platforms. The validation program ensures that hardware and software cryptographic implementations meet standard security requirements. Cryptography is a continually evolving field that drives research and innovation to deal with constantly advanced cryptanalysis techniques and rapidly growing computing powers for attackers. Furthermore, in today's digitalized environment, cryptographic mechanisms are implemented in a broader range of platforms for various purposes. The demand for new cryptographic tools has been higher than ever. The accomplishments below demonstrate NIST's continued dedication to the role it has fulfilled for nearly 50 years – leading public and private collaborations to foster continuous improvement and reliability in cryptographic techniques and technology.

Post-Quantum Cryptography (PQC)

In recent years, there has been steady progress in building quantum computers – machines that exploit quantum mechanical phenomena to solve problems that are difficult or intractable for conventional computers. When the capacity to build large-scale quantum computers exists, they will be able to break many of the public-key cryptosystems currently in use. This weakness would seriously compromise the confidentiality and integrity of digital communications on the Internet and elsewhere. The goal of post-quantum cryptography (PQC) (also called quantum-resistant or quantum-safe cryptography) is to develop cryptographic systems that are secure against quantum and classical computers and can also be deployed without drastic changes to existing communication protocols and networks.

The question of when a large-scale quantum computer will be built is a complicated one. In the past, it was less clear that large quantum computers were a physical possibility, but many scientists now believe it to be merely a significant engineering challenge. Some engineers even predict that, within the next 20 years, sufficiently large quantum computers will be built to break essentially all public-key schemes currently in use. Historically, it has taken decades to deploy modern public-key cryptography infrastructures, so efforts to prepare information security systems that are resistant to quantum computing must begin now.

Motivated by these considerations, NIST is in the process of selecting public-key (quantum-resistant) cryptographic algorithms through a public, competition-like process. The intent is for new public-key cryptography standards to specify one or more additional unclassified, publicly-disclosed digital signature, public-key encryption, and key-establishment algorithms. These algorithms will be available worldwide and capable of protecting sensitive government information well into the foreseeable future, including after the advent of quantum computers.

In Fiscal Year (FY) 2021, NIST continued evaluating the 15 algorithms still in the third round of analysis. NIST mathematicians and computer scientists consider these algorithms the strongest candidates for standardization. The list includes seven “finalists” for public-key encryption, key-establishment, and digital signature algorithms, as well as eight “alternates", which will likely need another round of evaluation. (The complete list is available on the NIST PQC website and is described in the *Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process*, NISTIR [NIST Interagency or Internal Report] 8309). In June 2021, NIST (virtually) held its third Post-Quantum Cryptography Standardization Conference. Each candidate team gave updates on their algorithms, and several researchers also presented their results.

In 2022, NIST expects to announce the algorithms that will be standardized and those that will be studied in a fourth round. NIST is also planning to issue a new Call for Proposals for public-key digital signature schemes to diversify its signature portfolio. This accomplishment represents several years of intensive research and industry collaboration. NIST appreciates the input of all submitters and those providing comments during the evaluation process.

Lightweight Cryptography

NIST has initiated a lightweight cryptography standardization process to solicit, evaluate, and standardize lightweight Authenticated Encryption with Associated Data (AEAD) and hashing schemes suitable for use in constrained environments where the requirements and performance of the currently approved NIST cryptographic algorithms are not acceptable. In August 2018, NIST published a Federal Register notice that specified the technical requirements for the target cryptographic algorithms and explained the evaluation criteria and a tentative timeline. The standardization process consists of multiple rounds, where, in each round, the field is narrowed to focus on the most promising candidates. In April 2019, NIST announced 56 first-round candidates, and after four months of evaluation, 32 of these candidates proceeded to the second round of evaluation.

The main goals of the standardization process during FY 2021 were to evaluate the security and performance of the 32 second-round candidates and to select the finalists that would advance to the last round of the evaluation. Additionally, NIST researchers continued to collaborate with the public at international conferences such as the *International Cryptographic Module Conference (ICMC 2021)*, the *2021 Security and Implementation of Lightweight Cryptography (SILC) Workshop*, the *Cryptographer's Track at the RSA Conference (CT-RSA)*, and the *Crypto 2021 Conference* that was organized by the International Association for Cryptologic Research (IACR).

NIST researchers performed software benchmarking using available implementations of the candidates, evaluated their performance on various microcontrollers, and compared them against the NIST AES-GCM and SHA-256 standards. (AES-GCM is the Advanced Encryption Standard algorithm with Galois Counter Mode. SHA-256 is the 256-bit Secure Hash Algorithm.) NIST researchers also published research results on the security of the candidates and design trends in lightweight cryptography.

NIST announced 10 finalists for the last round of evaluation in March 2021. Details of the selection process were published in the Status Report on the *Second Round of the NIST Lightweight Cryptography Standardization Process* (NISTIR 8369). This report included a summary of each second-round candidate and their main features, third-party security analysis, software benchmarking on microcontrollers, and hardware benchmarking results on various architectures.

NIST plans to host the Fifth Lightweight Cryptography Workshop in May 2022. After further security analysis and performance benchmarking of the finalists, NIST intends to select the winner and add a new cryptographic standard to NIST's portfolio.

Cryptographic Programs and Laboratory Accreditation

Cryptographic Security Testing laboratories are vital to ensuring that government systems protected by cryptography meet the validation requirements. There are currently 22 laboratories around the world certified through the National Voluntary Laboratory Accreditation Program (NVLAP). To better assess tester proficiency knowledge across all laboratories, the Cryptographic Validation Program (CVP) Certification Exam was revamped to update the older Federal Information Processing Standard (FIPS) 140-2 exam and incorporate the 2019 FIPS 140-3 standard's unique requirements.

Cryptographic Module Validation Program (CMVP)

When the use of cryptography is needed for the protection of sensitive unclassified information, federal agencies must use validated cryptographic modules. The Cryptographic Module Validation Program (CMVP) was created to support the federal user community's need for strong, independently tested, and commercially available cryptographic modules. Working with U.S. and Canadian agencies, NIST has incorporated standards from international organizations that represent both public and private sectors within the cryptographic community.

To assist the community, the CMVP put a process in place by which labs/vendors could request an extension until March 31, 2022 for submission of FIPS 140-2 reports that could not meet the previously specified September 2021 deadline. Until that deadline, the CMVP is managing a dual validation process for both FIPS 140-2 and FIPS 140-3 validations. Over 300 FIPS 140-2 certificates have been awarded in FY 2021. The first FIPS 140-3 submissions are being reviewed, and only FIPS 140-3 submissions for new validations will be accepted after March 31, 2022.

A number of elements of the current validation processes are manual in nature, and the period required for third-party testing and government validation of cryptographic modules is often incompatible with industry requirements. Federal users and others who depend on validated cryptography face a dilemma when frequent updates and patches are essential for staying ahead of attackers, but the existing CMVP validation process does not permit rapid implementation of these updates while maintaining a validated status. NIST has started a broad effort through the National Cybersecurity Center of Excellence (NCCoE) to modernize and automate its cryptographic validation programs. The purpose of the project is to demonstrate the value and practicality of automation to improve the efficiency and timeliness of the CMVP operation and processes. This project will demonstrate a suite of tools to modernize and automate manual review processes in support of existing policy and efforts to include CMVP technical testing.

The CMVP has partnered with the Cryptographic Module Users Forum (CMUF) to identify areas of change that make interpreting the standards difficult. The CMVP is also working with the CMUF to minimize communications confusion between vendors and the laboratories and between the laboratories and the CMVP. These improvements are captured in publicly available supporting documents and standards. Through this work, NIST will identify ways to make the process more efficient and faster for vendors, laboratories, and the CMVP while providing assurance of correct implementation.

Cryptographic Algorithm Validation Program (CAVP)

The Cryptographic Algorithm Validation Program (CAVP) continued to perform algorithm validations with the NIST-hosted Automated Cryptographic Validation Test System (ACVTS). The program has offered more than 435,000 algorithm tests over FY 2021 on a test-only demonstration server and a validation production server.

Entropy source validation has been a focus of the validation programs over the past year. Many discussions were held with the cryptographic validation community to determine the best way to meet the needs of NIST, the validation authority, and the entropy source developers and testers. Additional documentation and instructions on how to cite conformance to the *Recommendation for the Entropy Sources Used for Random Bit Generation* (SP 800-90B) has been provided and will continue to be provided in FY 2022. Additionally, based on the success of the ACVTS, a new server has been developed called the Entropy Source Validation Test System. This system will collect information on SP 800-90B-compliant entropy sources in order to issue validations on a new entropy source validation list. The system is expected to be made available in 2022.

2 | Cybersecurity Measurement

Credit: Shutterstock

Every organization wants to gain maximum effect and value for its finite cybersecurity-related investments. This includes managing risk to the enterprise and optimizing the potential reward of cybersecurity policies, programs, and actions. Organizations frequently make decisions by comparing various projected costs with potential associated benefits and risk-reduction scenarios. Senior executives need accurate and quantitative methods to portray and assess these factors, their effectiveness and efficiency, and their effect on risk exposure. Providing reliable answers to these questions requires organizations to employ a systematic approach to cybersecurity measurement that considers current knowledge limits.

NIST's cybersecurity measurements program enables organizations to manage cybersecurity risks by supporting the development and alignment of technical measures to determine the effect of cybersecurity risks and responses on an organization's objectives. A mature metrics program is content-rich, supports a broad range of stakeholders, and provides greater value to the organization. More precise measurement data helps organizations focus on an actionable approach to improving cybersecurity. NIST's various initiatives to support this effort include research in new technology areas and the development of risk management tools, test resources, guidance, and ways for organizations to continue to mature their use of cybersecurity metrics. These initiatives involve collaboration with the research, business, and government sectors.

Cyber Risk Analytics (CRA)

The CRA project promotes technical solutions and guidance to improve the understanding of cybersecurity risks, inform management practices, and facilitate information sharing among risk owners. NIST is leveraging past and present efforts, such as using a data repository for cyber incident analysis, predictive analytics and strategic analysis on threat coverage, prioritization and gap identification. In FY 2021, the research explored natural language processing to provide added enrichment and enhanced graph visualization to cyber incident data in a collaborative repository. The ability to measure an enterprise's software flaws and misconfiguration is vital, yet that vulnerability state cannot be measured if those flaws are undiscovered or undisclosed. CRA contributed to the draft of the *Recommendations for Federal Vulnerability Disclosure Guidelines* (SP 800-216). The guidance gives recommendations on the disclosure process for security vulnerabilities of information systems in response to the Internet of Things Cybersecurity Improvement Act of 2020. CRA also collected and adjudicated public comments and initiated the research to update the *Performance Measurement Guide for Information Security* (SP 800-55, Revision 1).

Software Assurance Metrics and Tool Evaluation (SAMATE)

The SAMATE project conducted by the Software and Systems Division (SSD) is dedicated to improving software assurance by developing methods to enable software tool evaluations, measuring the effectiveness of tools and techniques, and identifying gaps in the available tools and methods. Major efforts include defining software error classes (software bugs), compiling a list of programs with known bugs, and enabling a better understanding of tool effectiveness.[1] In FY 2021, NIST Information Technology Laboratory (ITL) published *Guidelines on Minimum Standards for Developer Verification of Software* (NISTIR 8397). Developed in consultation with others at NIST, National Security Agency (NSA), and numerous outside organizations, this report responded to a portion of Executive Order (EO) 14028, *Improving the Nation's Cybersecurity.*

- *The Bugs Framework (BF)* is a language-independent classification of software bugs and weaknesses that allows precise descriptions of vulnerabilities that exploit them. In FY 2021, NIST published the Input/Output Check Bugs Model, the Data Validation Bugs class (which also defines five types of Injection Errors), and the Data Verification Bugs class.
- *The Software Assurance Reference Dataset (SARD)* is an extensive collection of programs with precise software bug types and locations. The programs are in C, C++, Java, PHP, and C#, covering over 150 classes of weaknesses. In FY 2021, NIST produced a beta version of redesigned SARD, which has enhanced capabilities.
- *Static Analysis Tool Exposition (SATE)* advances research in static analysis tools that find security-relevant weaknesses in source code. NIST provides a set of programs to toolmakers, and they run their tools and return tool outputs for analysis. In FY 2021, NIST continued the analysis of tool outputs for SATE VI.

Automated Combinatorial Testing (ACT)

ACT research is focused on the application of combinatorial methods for the measurement and assurance of artificial intelligence (AI) and machine learning (ML) systems. The NIST ACT research team developed a new method and tool for analyzing and explaining the decisions of AI/ML algorithms and presented this research to U.S. Air Force and U.S. Army researchers. The project team has also collaborated with Virginia Tech on transfer learning problems and applications of combinatorial methods to assured autonomy. Under an interagency agreement with NASA (National Aeronautics and Space Administration), this research will be applied to advanced air mobility.

[1] Classes and description of the Bugs Framework are described at https://csrc.nist.gov/CSRC/media/Presentations/Foundations-of-Software-Assurance/images-media/3_software-assurance_pblack.pdf

Computer Forensic Tool Testing (CFTT)

In FY 2021, the CFTT Program, a project supported by NIST's Special Programs Office and the Department of Homeland Security (DHS), helped address critical needs in the law enforcement community to ensure the reliability of computer forensic tools to identify and store evidence from a computing device.

- *Specifications and Testing* – the CFTT partnered with DHS to test numerous digital forensic tools for search functions, mobile device acquisition, and SQLite Data Recovery, resulting in 12 published reports.
- *Federated Testing* – Federated testing was developed to provide third parties with the ability to use the NIST testing methodology in their labs and produce standardized test reports. In FY 2021, NIST added a new test suite, Federated Testing Lite, for string searching and mobile forensics data.
- *Computer Forensic Reference Data Sets (CFReDS)* – The CFReDS project is a repository of various documented sets of digital evidence. In FY 2021, an improved CFReDS portal was published and is currently live at https://cfreds.nist.gov/. The goal is for the CFReDS website to be a centralized portal that provides the forensic community with a quick and easy way to find and share datasets of interest.
- *Forensics Tool Catalog* – The Forensics Tool Catalog is a web-based, community-sourced catalog of software forensics tools aided by a taxonomy. In FY 2021, the catalog entries increased to 208 entries from 82 vendors.

National Software Reference Library (NSRL)

The NSRL collects software from various sources and incorporates the file profiles computed from this software into a Reference Data Set (RDS) of information. The RDS is used by law enforcement, government, and industry to review computer files by matching file profiles in the RDS. This will help alleviate much of the effort involved in determining which files are important as evidence on computers or other electronic devices that have been seized as part of criminal investigations. The NSRL also provides a research environment to promote the development of new forensics techniques and other applications in computer science.

In FY 2021, the NSRL published four releases of software metadata and enlarged the collection to contain 897 million files from 43,629 microcomputer applications; 198,321 mobile device applications; and 3,897 gaming platform applications.

3 | Education and Workforce

Credit: Shutterstock

NIST continues to coordinate a National Cybersecurity Awareness and Education Program, as required by the Cybersecurity Enhancement Act of 2014 that includes activities such as:

- The widespread dissemination of cybersecurity technical standards and best practices;
- Efforts to make cybersecurity best practices usable by a variety of individuals and stakeholders;
- Increasing public awareness of cybersecurity, cyber safety, and cyber ethics;
- Increasing understanding of the benefits of ensuring effective risk management of information technology and the methods to mitigate and remediate vulnerabilities;
- Supporting formal cybersecurity education programs at all levels to prepare and improve a skilled cybersecurity workforce; and
- Promoting initiatives to evaluate and forecast future cybersecurity workforce needs of the Federal Government and develop strategies for recruitment, training, and retention.

National Initiative for Cybersecurity Education (NICE)

The mission of NICE is to energize, promote, and coordinate a robust community that works together to advance an integrated ecosystem of cybersecurity education, training, and workforce development. The NICE Strategic Plan, released in November 2020, introduces five new strategic goals, each with a set of objectives. To more closely align with the new Strategic Plan, updates were also made to NICE's public working group structure, which is now called the NICE Community Coordinating Council. The Council consists of three working groups that are aligned to strategic goals and four communities of interest aligned to priority topic areas. Early in 2021, the NICE Program Office and NICE Community Coordinating Council began work on drafting an Implementation Plan for the new Strategic Plan. The Implementation Plan was published in September 2021.

In FY 2021, there were also several activities surrounding the NICE Framework. In November 2020, NIST published a framework update – *Workforce Framework for Cybersecurity* (SP 800-181, Revision 1). Competencies were reintroduced in the revision, and subsequently, a draft *NICE Framework Competencies: Assessing Learners for Cybersecurity Work* (NISTIR 8355) and a draft list of competencies were released for public comment. In addition, three workshops were held in FY 2021 to explore areas in which the NICE Framework could be expanded: Competencies: Moving from Concept to Implementation (March 2021), Developing a Workforce to Secure Operational Technologies (August 2021), and Developing a Workforce for Security Awareness and Behavior Change (September 2021). Finally, NIST released eight NICE success stories. These articles demonstrate how an organization has used the NICE Framework and emphasize the drivers, process, and outcomes – including benefits and lessons learned – to help improve an understanding of the NICE Framework. These success stories also promote ideas on how to adopt the framework and associated products.

Federal Cybersecurity Workforce

NIST has brought together the federal cybersecurity community throughout the year through two major programs: the Federal Cybersecurity Workforce Summit/Webinars and the Federal Information Security Educators (FISSEA). In addition to the Federal Cybersecurity Workforce Summit, which covered topics such as national cybersecurity priorities and policy initiatives and the strategic vision for the federal cybersecurity workforce, a webinar was held to share assessment policies, strategies, and practices for cybersecurity hiring. Additionally, FISSEA's Summer and Fall forums brought together Federal Government information security professionals to explore techniques for awareness and training. FISSEA also recognized two innovators of the year and several winners in a contest for best awareness and training materials, including blogs, posters, and more.

Advancing Cybersecurity Usability

The NIST Usable Cybersecurity team conducted research to better understand the factors that influence youth cybersecurity and privacy knowledge and behaviors across both the home and school contexts. At the 2021 USENIX Security Symposium, NIST published the results from a large-scale survey of 1,505 3rd to 12th graders from schools across the United States. In preparation for a future report, the team also analyzed data from a study of passwords used by parents. NIST also conducted an interview study with parent/child pairs to understand youth perceptions of online security and privacy and potential parental influences. Research results will inform efforts to provide guidance and best practices to youths, their parents, and educators so that youths can stay safe and secure online while enjoying the benefits of the Internet.

NIST also completed a study to understand the needs, challenges, practices, and competencies of federal security awareness professionals and programs. The results of the study will inform the creation of resources for federal programs, including examples of successful practices and the lessons learned. Findings were presented to federal security forums and are directly contributing to the NICE Cybersecurity Workforce Framework and a revision of NIST Special Publications related to security awareness and training programs. Multiple reports detailing the results will be published in 2022.

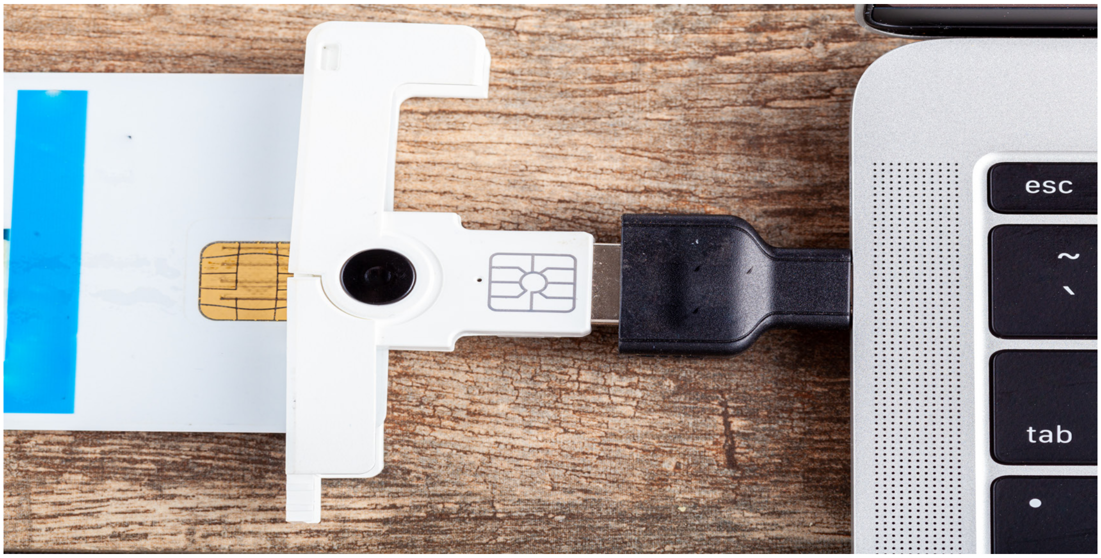
Small Business Cybersecurity Corner

In FY 2021, the Small Business Cybersecurity Corner website, which provides cybersecurity basics, guidance, solutions, and training for keeping a small business secure, was updated to include the latest materials from NIST and other federal partners that are appropriate for small and medium-sized business (SMB) owners. Some examples include the addition of new "quick start" guides for both the NIST Cybersecurity Framework and NIST Privacy Framework. For example, the Guidance by Topic section of this website includes topic-specific guidance on actions to take to address cybersecurity risks and secure a business. This section was updated during FY 2021 to include the latest cybersecurity topics, such as detailed instructions on protecting a small business from ransomware and phishing attacks.

A series of "case studies" was created to enable a small business to educate its employees about common cybersecurity risks. Each case study is limited to a single printable page and is designed to provide sufficient information to allow a discussion of the topic's relevance to the organization. The topics include phishing, social engineering, keystroke logging, encryption, and data breaches.

In late FY 2021, planning began for a series of SMB-focused videos to explain the most common cybersecurity risks to small businesses and ways to stay protected. Each video will be hosted on a dedicated topic page on the Small Business Cybersecurity Corner website.

4 | Identity and Access Management



Credit: Shutterstock

Identity and Access Management (IdAM) is a fundamental and critical cybersecurity capability to ensure that the right people and things have the appropriate access to the proper resources at the right time. To advance the state of IdAM, NIST:

- Conducts focused research to better understand new and emerging technologies, impacts on existing standards, and ways to implement IdAM solutions;
- Leads in the development of national and international IdAM standards, guidance, best practices, profiles, and frameworks to create an enhanced, interoperable suite of secure, privacy-enhancing solutions;
- Evolves its IdAM standards, guidelines, and resources; and
- Produces example solutions that bring together the IdAM requirements needed to address specific business cybersecurity challenges.

IdAM is an important component of cloud computing security, and NIST publishes access control characteristics and general access control guidelines for various cloud service models. NIST also performs research and development regarding access control rules and methods.

Personal Identity Verification (PIV)

As required by Homeland Security Presidential Directive 12, NIST developed and maintains FIPS 201 for the personal identity verification (PIV) of federal employees and contractors. In FY 2019, NIST initiated a revision of FIPS 201 to incorporate the changing business requirements of federal departments and agencies and to adapt to an evolving technology environment. Revision activities began in FY 2019 with a business requirement meeting to engage with federal stakeholders about the revision goals.

In FY 2020, the PIV team updated the draft standard based on the revision goals and published a public draft of FIPS 201. Comments received were adjudicated in FY 2021 and subsequently reflected in the final FIPS 201. The standard expands the set of PIV authenticators beyond the current practices (including the current smart card form factor) while addressing the interagency use of new types of PIV authenticators (i.e., derived PIV credentials) via federation. The revision also aims to facilitate the issuance of PIV cards by enabling remote identity proofing. These changes closely align with Office of Management and Budget (OMB) Policy Memorandum M-19-17, *Enabling Mission Delivery through Improved Identity, Credential, and Access*. For FY 2022, the PIV team will actively work on Special Publications associated with FIPS 201 to further specify the standard's technical details while continuing outreach to federal stakeholders.

Digital Identity Guidelines

The four-volume set of *Digital Identity Guidelines* (NIST SP 800-63-3) was published in June 2017. Following three years of federal agency experience implementing the controls and requirements and recognizing the need to stay ahead of online identity attacks, ITL revised and updated all volumes of SP 800-63-3 in June 2020.

In June 2020, NIST also published the pre-draft Request for Comments for the anticipated revision of SP 800-63-3. The Request for Comments identified topics for potential updates, and more than 40 federal agencies and industry organizations responded with over 300 comments to the request. ITL subsequently published a public roadmap for key activities, milestones, and target dates for the development of SP 800-63 Revision 4, and published all comments received by the comment closing date. As indicated in the roadmap, ITL completed the adjudication of comments received in the first and second quarters of FY 2021. ITL posted six SP 800-63, Revision 4 topic items for additional discussion in February 2021 to present revisions for consideration. The discussion items encouraged federal agency and industry feedback and discussion on the prospective revisions. The open discussion period ended in May 2021. ITL anticipates publication of draft SP 800-63, Revision 4 in the third fiscal quarter of 2022.

With the publication of the third set of conformance criteria for *Federation and Assertions* (SP 800-63C), following on the release of conformance criteria for volumes SP 800-63A and SP 800-63B in June 2020, the full set of conformance criteria for all volumes of SP 800-63-3 has been completed. The conformance criteria present all normative requirements and controls for the SP 800-63A, B, and C and provide supplemental guidance, control objectives, and recommended test and conformance assessment methods for all of the normative requirements and controls at the designated assurance levels. The conformance criteria are used by federal agencies, independent assessment and certification bodies, auditors, and implementers so that all of the normative requirements and controls for SP 800-63-3 are understood for proper implementation, conformance assessment, and audit.

Mobile Driver's License

NIST contributed to the development of an international standard for mobile drivers licenses (mDL). The mDL is a secure digital representation of DL data that is provisioned onto a smart mobile device, such as a smart phone or tablet, for use by the proper, intended mDL Holder. It can also contain information relevant to additional state privileges or national context. The standard was developed in coordination with other countries and with the cooperation of identity management experts from around the world. The standard provides a specification for an interoperable interface between the reader device and mDL. As is currently the practice with the physical license document, an mDL can now be presented to a human or digital verification authority in exactly the same way using a mobile device. The standard defines what is known as "mdoc" (mobile documents) technology. The standard is not limited to drivers licenses and is a launching pad for other identity documents/cards, such as passports, travel documents, birth certificates, voting registration/cards, vaccination cards, and organization identity cards.

Subsequent to the publication of the standard, NIST created an mDL reader device reference implementation, which is used to test vendor mDL instances and enable relying parties to apply mDL in their systems.

Access Control Policy Verification and Development Tools

Traditional access control policy verification methods have capability and performance issues related to inaccuracy and complexity that is limited by applied technologies. For instance, model proof, test oracle, and data structure methods initially assume that the policy under verification is faultless unless the policy model cannot handle test cases. Thus, the challenge of the method is to compose test cases that can comprehensively discover all faults. Alternatively, a system simulation method requires translating the policy to a simulated system. The translation between systems may be difficult or impractical to implement if the policy logic is complicated or the number of policy rules is large. To answer these challenges, *Machine Learning Method for Access Control Policy Verification* (NISTIR 8360) proposes an efficient and straightforward method for access control policy verification by applying a classification algorithm of machine learning that does not require comprehensive test cases, oracle, or system translation but rather checks the logic of policy rules directly, making it more efficient and feasible compared to traditional methods.

Attribute-based Access Control for Microservices-based Applications

Cloud-native applications now consist of loosely coupled components called microservices (typically implemented as containers), with all application services (e.g., authentication, authorization, load balancing, setting up of network connections) provided through a dedicated infrastructure called the service mesh, which is independent of the application code. The requirements of the authorization service in this environment are to build the following:

- The concept of zero trust by enabling all authorizations for every application request to be based on a verification of the identity of the user, service, or device irrespective of the location or nature of the requesting service; and
- A robust access control mechanism based on an expressive access control model, such as Attribute-based Access Control (ABAC), that can be used to express a wide set of policies based on a rich set of all contextual attributes and is scalable in terms of the user base, objects (resources), and deployment environment.

Attribute-based Access Control for Microservices-based Applications Using a Service Mesh (SP 800-204B) was published in August 2021. This publication provides guidance for building an ABAC-based deployment within the service mesh that meets the requirements stated above. The security assurance provided by the deployment, the supporting infrastructure needed, and the advantages of Next Generation Access Control (NGAC) – the ABAC model representation developed at NIST that is used in the deployment – are also discussed.

5 | Privacy Engineering

Credit: Shutterstock

The Privacy Engineering Program (PEP) works to provide trusted, rigorous tools and resources that support innovation and privacy. PEP facilitates dialogue among stakeholders about privacy risk management and promotes an organizational shift away from checklist-based legal compliance to improve privacy measures. The following activities reflect progress made in FY 2021 toward three strategic PEP objectives: advancing the development of privacy engineering and risk management guidelines and resources, positioning NIST as a leader in privacy research, and advancing the development and deployment of privacy-enhancing technologies.

Privacy as a programmatic area intersects with each of the other priority focus areas, making coordination and ongoing engagement critical across a range of technical domains. To advance its strategic objectives, PEP collaborates with other NIST programs, including the NCCoE, the Cryptographic Technologies Group, the Federal Information Security Modernization Act (FISMA) program, and the Cybersecurity for the Internet of Things (IoT) Program, as reflected in activities throughout this report.

Privacy Framework

NIST continued its Privacy Framework outreach and awareness efforts in FY 2021 in numerous domestic and international speaking engagements at conferences, webinars, and podcasts. NIST also worked closely with stakeholders to develop resources and guidelines to assist with Privacy Framework publication, with a focus on an audience of small and medium businesses (SMBs) and other organizations with limited privacy resources. In January, NIST released new resources to coincide with its one-year anniversary celebration. These included a Quick Start Guide for SMBs and an animated video to introduce the Privacy Framework to a general audience.

NIST stakeholders made significant and helpful new contributions to the online resource repository. These contributions included new regulatory crosswalks to key domestic and international privacy regulations and translations of the Privacy Framework to Spanish, Portuguese, and Bahasa Indonesia. A broad group of implementers voiced their support for the Framework by contributing 14 new quotes to the Privacy Framework website. In early 2022, NIST plans to release its first Privacy Framework "Success Story", which will be provided from the Arlington County, Virginia government.

Workforce Advancement

In April 2021, NIST officially launched a Privacy Workforce Public Working Group (PWWG) pursuant to the Privacy Framework companion roadmap and in response to stakeholder challenges with privacy workforce recruitment and development. The PWWG provides a forum in which participants from the general public – including private industry, the public sector, academia, and civil society – can create descriptions of tasks, knowledge, and skills aligned with the Privacy Framework Core Subcategories and the NICE Cybersecurity Workforce Framework taxonomy to support the development of a workforce capable of managing privacy risk. The PWWG currently has over 600 members from across the world and has two active project teams generating the PWWG work product.

Privacy Leadership

Through leadership positions in key privacy and security organizations, NIST helps drive change and the standardization of privacy considerations. NIST personnel co-chaired the Interagency Working Group (IWG) for Privacy with the U.S. Networking and Information Technology Research and Development (NITRD) Program, co-chaired the NIST Privacy Workforce Public Working Group, and served as the first privacy co-chair of the Federal Computer Security Managers' Forum (FCSM).

Privacy-Enhancing Technologies

NIST continues its work in advancing the understanding and deployment of privacy-enhancing technologies. In FY 2021, there has been increased interest among federal agencies in the use of these technologies to enable greater research access to agency datasets while maintaining security and privacy. In May 2021, NIST co-hosted a workshop with the National Science Foundation (NSF) on this topic. As a follow-up to the workshop, NIST has been working with the NSF to develop a prize challenge to accelerate the use of these technologies, which is anticipated to be announced in FY 2022.

Differential Privacy

Differential privacy involves adapting a dataset that has personal information in it such that the personal information is not readily identifiable. In FY 2021, NIST produced a blog series about differential privacy and applicable use cases and to help privacy engineers and Information Technology (IT) professionals that covers the basics, applicable use cases, and open-source tools available for an implementation to leverage the differential privacy contributions indexed in the Privacy Engineering Collaboration Space (an online venue open to the public where practitioners can discover, share, discuss, and improve upon open-source tools, solutions, and processes that support privacy engineering and risk management).

The series is designed to help business process owners and privacy program personnel understand basic concepts on how to implement the tools. Anticipated to be completed in early FY 2022, the series will serve as a foundation for the development of a technical guideline for deploying differential privacy.

Privacy-Enhancing Cryptography

The Privacy-Enhancing Cryptography project promotes the use of cryptographic protocols that enable parties to interact meaningfully without revealing private information to one another or to third parties. Toward this end, NIST has been engaged with various stakeholders, researchers, and developers. In FY 2021, motivated by the need to conduct automated exposure notification related to the current pandemic, NIST developed a privacy-protecting method to measure levels of interaction within a population. NIST also launched a quarterly series of talks on topics related to privacy and public auditability.

6 | Risk Management

Credit: Shutterstock

Throughout FY 2021, NIST has made significant progress in advancing methods and guidelines for managing enterprise risk related to cybersecurity, systems engineering, and privacy. NIST is leading a multi-year effort to produce a cohesive portfolio of complementary risk management resources that can be used individually or together to help public and private organizations better manage technology and data risk under the established umbrella of enterprise risk management (ERM).

Risk management has been a fundamental driver for organizations for as long as there have been information and operations to protect. Today's proliferation of risk management resources, combined with advances in technology, increasingly calls for a collaborative approach to managing discipline-specific risks within the enterprise. This includes the need to ensure that executives, fiduciaries, managers, risk professionals, developers, and designers work together to manage risk through established methods of risk management.

Risk Management Framework Updates

NIST continues to update guidance and develop new resources to support the implementation of the NIST Risk Management Framework (RMF) as described in SP 800-37, Revision 2. In FY 2021, NIST published *Managing the Security of Information Exchanges* (SP 800-47, Revision 1). This publication provides guidance on identifying information exchanges, considerations for protecting exchanged information, and the agreement(s) needed to help manage the protection of the exchanged information. The latest update of SP 800-47 focuses on managing the risk associated with the information being exchanged or accessed before, during, and after the exchange rather than on any type of technology-based connection or information access/exchange method.

NIST also published *ISCMA: An Information Security Continuous Monitoring (ISCM) Program Assessment* (NISTIR 8212). NISTIR 8212 provides an example operational approach to the ISCM program assessment described in *Assessing Information Security Continuous Monitoring*

Programs: Developing an ISCM Program Assessment (NIST SP 800-137A). The ISCMAx software tool – a free, publicly available working implementation of ISCMA – can be tailored to fit the needs of any organization. The NISTIR 8212 includes instructions for using ISCMAx and for tailoring it if desired.

The NIST RMF website was redesigned and expanded to include additional introductory materials, new resources to support implementers, and improvements to usability and user experience. New website features include the SP 800-53 Security and Privacy Controls and Baselines Search (Release Search) and the SP 800-53 Downloads pages. The Release Search provides a browser-based version of the SP 800-53 controls and SP 800-53B control baselines to allow users to quickly access, search, and use the controls and baselines. The SP 800-53 Downloads page offers the controls, baselines, and SP 800-53A assessment procedures for downloading in multiple data formats, including Extensible Markup Language (XML), portable document format (PDF), comma-separated value (CSV), spreadsheet, and Open Security Control Assessment Language (OSCAL).

To promote and increase stakeholder engagement for the development of SP 800-53, NIST released an online tool to allow real-time input about controls and control baselines. This tool, the NIST SP 800-53 Controls Public Comment Site, is a model for how standards and guidelines can keep pace with changes in technology and society, encourage all stakeholders to participate in the NIST publication development and review process, and modernize how certain types of publications are issued in a more user-friendly manner.

Protecting Controlled Unclassified Information

Controlled unclassified information (CUI) is routinely shared with nonfederal organizations—state and local governments, universities, research organizations, and the private sector—and must be protected by the nonfederal organization. In FY 2021, NIST developed new guidelines to protect CUI in critical programs and systems from advanced persistent threats (APTs). *Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171* (SP 800-172) offers additional recommendations for handling CUI in situations where that information runs a higher than usual risk of exposure. The enhanced security requirements protect the confidentiality, integrity, and availability of CUI from APTs by promoting penetration-resistant architectures, damage-limiting operations, and designs to help achieve cyber resiliency and survivability. NIST also issued *Assessing Enhanced Security Requirements for CUI* (draft SP 800-172A) to assist organizations with planning and conducting efficient, effective, and cost-effective assessments of the enhanced security requirements in SP 800-172.

Integration of Cybersecurity Risk Management into ERM

Information and technology are among the most valuable resources to each enterprise, so it is important that cybersecurity risk management be well integrated with other elements of enterprise risk management (ERM). Building on the foundation of *Integrating Cybersecurity and Enterprise Risk Management* (NISTIR 8286), which was released in 2020, NIST has created a series of publications to provide ways to better align enterprise risk considerations with cybersecurity risk activities at all organizational levels. The three reports are described below:

- NISTIR 8286A details the context, scenario identification, and analysis of the likelihood and impact of cybersecurity risk. It also includes methods to convey risk information, such as cybersecurity risk registers (CSRRs) and risk detail records.

- NISTIR 8286B describes ways to apply risk analysis to help prioritize cybersecurity risk, evaluate and select appropriate risk responses, and communicate risk activities as part of an enterprise cybersecurity risk management strategy.

- NISTIR 8286C describes the processes for aggregating information from cybersecurity risk management (CSRM) activities throughout the enterprise. As that information is integrated and harmonized, organizational and enterprise leaders monitor the achievement of risk objectives, consider any changes to risk strategy, and use the combined information to maintain awareness of risk factors and positive risks (or opportunities).

By ensuring that cybersecurity decisions are based on enterprise leaders' expectations and by ensuring effective communication at all levels (such as through the use of the CSRR), risk management activities throughout the enterprise can be conducted in a more consistent manner and will remain well aligned with enterprise objectives.

Advancing the Application of the NIST Cybersecurity Framework

NIST has continued to foster the adoption and application of the *Framework for Improving Critical Infrastructure Cybersecurity* (NIST Cybersecurity Framework, Version 1.1). NIST has participated in a range of public events to develop and assist users in using the NIST Cybersecurity Framework. Due to the COVID-19 pandemic, those events were held virtually and included a cybersecurity risk management webinar series that was co-hosted by the Center for Cybersecurity Policy and Law.

NIST helps organizations use the Cybersecurity Framework by developing sector-specific resources and by documenting the relationships among many NIST and non-NIST resources. Additionally, NIST released a *Cybersecurity Framework Quick Start Guide* (NIST SP 1271) to help any organization seeking to improve cybersecurity risk management by using the Cybersecurity Framework.

The NIST Cybersecurity Framework website continues to expand with learning materials, success stories, and other helpful resources. In 2021, NIST developed a specific website for international cybersecurity and privacy resources that includes information on translations and adaptations of the Cybersecurity Framework as well as ongoing international engagement and relevant standards development efforts. This has contributed to progress in encouraging a global use of the framework and interoperability with other cybersecurity models. The website now contains translations of the framework into Arabic, Bulgarian, Indonesian, Japanese, Polish, Portuguese, and Spanish.

NIST also contributes to international standards development efforts related to cybersecurity risk management and the development of cybersecurity frameworks, including the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) Technical Specification 27110:2021, *Information technology, cybersecurity, and privacy protection – Cybersecurity framework development guidelines*, that was published in 2021. This document specifies guidelines for developing a cybersecurity framework and notes that all cybersecurity frameworks should have the following concepts that align with the Cybersecurity Framework's five functions: Identify, Protect, Detect, Respond, and Recover.

Cybersecurity Supply Chain Risk Management (C-SCRM) Program

NIST continued work on the Cybersecurity Supply Chain Risk Management (C-SCRM) program. C SCRM is the process of identifying, assessing, and responding to risks associated with the distributed and interconnected nature of information, communications, and operational technology product and service supply chains. C-SCRM is integrated into systems security engineering (SSE) and covers the entire system life cycle (including research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal) since supply chain threats and vulnerabilities may (intentionally or unintentionally) compromise a technology product or service at any stage.

In FY 2021, NIST launched the National Initiative for Improving Cybersecurity in Supply Chains (NIICS). The initiative will rely on private companies of all sectors and sizes, as well as government and academia, to contribute to the development of usable and effective domestic and global supply chain risk management practices. The process aims to reflect lessons learned from the past and current joint efforts to improve the way in which cybersecurity risks are managed – especially as they relate to supply chains involving smaller organizations, which frequently face special cybersecurity-related challenges. From the outset, NIST will include a special focus on promoting the development and adoption of international standards that will lead to the global use of the approaches and solutions developed as a result of this partnership.

NIST served as a principal member of the Federal Acquisition Security Council (FASC), which was created as a requirement of the Federal Acquisition Supply Chain Security Act of 2018 (FASCSA). In addition, NIST participated in the FASC policy working group and FASC task force and assisted in the development and finalization of the FASC rule (41 CFR Part 201). The FASC and its subsidiary bodies are responsible for the development of policies and processes for agencies to use when purchasing technology products. It also recommends C-SCRM standards, guidelines, and practices that NIST should develop. Ongoing participation in the C-SCRM Forum enabled important discussions among many of those leading C-SCRM efforts in the federal ecosystem. These discussions helped to prepare participants for many of the supply chain risk events that federal stakeholders have recently faced.

NIST initiated its first major revision to its foundational supply chain risk management guidance, publishing the initial public draft of *Cybersecurity Supply Chain Risk Management (C-SCRM) Practices for Systems and Organizations* (SP 800-161, Revision 1) in April 2021. This revision provides organizations with updated guidance for mitigating cybersecurity risks in the supply chain and provides a directional roadmap for agencies to follow to aid them in developing and growing their C-SCRM capabilities. It lays out a set of foundational practices to build a sustainable program and, over time, mature and evolve to incorporate enhanced capabilities. The publication emphasizes the importance of an inter-disciplinary and cross-organizational approach to C-SCRM grounded in governance, accountability, and responsibility. Ensuring that supply chain risk is addressed throughout the entirety of the life cycle of a product or system and across all procurement and contract management phases is a core theme throughout the guidance.

NIST also includes expansive, updated guidance for supply chain security controls that can be selected, tailored, and implemented to mitigate cybersecurity risks in the supply chain and risks inherited from and inherent in acquired products and services. The publication instructs organizations on the activities and roles involved in the supply chain risk management process; provides templates to aid them in their development of internal C-SCRM policy, strategy, and implementation plans; and highlights and describes a number of factors (addressing C-SCRM in acquisitions, the importance of information sharing, having sufficient resources, investing in training, and measuring progress and outcomes) that are critical to the successful implementation and effectiveness of a C-SCRM Program.

The second public draft of the publication was released in October 2021. Two new significant appendices were added in this second draft. The “FASCSA Appendix” provides agencies with additional guidance concerning specific requirements outlined in the FASCSA. This appendix provides guidance on the prioritization of supply chain risk assessments, establishes baseline risk factors to bring greater consistency and alignment between agency-level and government-wide C-SCRM risk assessment and response functions, and introduces a supply chain risk severity schema that can be used to guide referrals of significant risk to the FASC for further review, decision, and action as needed. The second new appendix provides preliminary guidelines for enhancing software supply chain security and was developed in response to EO 14028, *Enhancing the Nation’s Cybersecurity*. This appendix outlines existing software supply chain security industry standards, tools, and recommended practices within the context of the draft of SP 800-161, Revision 1. Final publication is anticipated to be released during the third quarter of FY 2022.

An NCCoE demonstration project identified methods by which organizations can verify that their purchased computing devices are genuine and have not been altered during the manufacturing and distribution processes. In addition, the NCCoE released the Preliminary Draft of *Validating the Integrity of Computing Devices* (NIST Cybersecurity Practice Guide SP 1800-34, Volumes A, B, and C).

Cybersecurity for the Internet of Things (IoT) Program

The Cybersecurity for IoT Program’s FY 2021 efforts primarily occurred in three areas: continuing to build out a suite of guidance for manufacturers of IoT devices; efforts to develop guidance for consumer IoT cybersecurity, including responding to the requirements of the President’s Executive Order (EO) 14028; and addressing the requirements of the IoT Cybersecurity Improvement Act of 2020 to provide cybersecurity guidance for federal agencies that are using IoT devices.

The development of guidance for manufacturers expanded upon the previously published *IoT Device Cybersecurity Core Baseline* (NISTIR 8259A). Early in FY 2021, NIST published a public review draft of *IoT Non-technical Supporting Capability Core Baseline* (draft NISTIR 8259B). This document complements NISTIR 8259A’s technical requirements with a baseline of non-technical activities that manufacturers and their supporting third parties should undertake in order to support their customers in securely deploying and operating their products. The draft of NISTIR 8259B served as the starting point for a series of stakeholder interactions that included meetings with industry groups and organizations, a workshop in April 2021 and a series of roundtables in June 2021. These interactions enabled the program to publish the final version of NISTIR 8259B in August 2021 and make substantial progress toward a federal guideline publication that is anticipated for release in FY 2022. NISTIR 8259B was also added to NIST’s Online Informative References (OLIR) program database as a focal document.

In parallel with these efforts, the IoT Cybersecurity Program continued refining a detailed catalog of technical cybersecurity capabilities and non-technical supporting capabilities that expand on the NISTIR 8259A and 8259B baselines. The online catalog presentation was refactored to be more usable. The program received considerable feedback that guided catalog improvements. The capabilities in the catalog were also mapped to NIST SP 800-53, Revision 5 and to the NIST Cybersecurity Framework to better connect the program’s activities with broader NIST guidance on risk management. The program supported activities within the NCCoE to document the alignment of its work with that of NIST.

Efforts related to consumer IoT cybersecurity started with an October 2020 virtual workshop on Cybersecurity Risks in Consumer Home IoT Products that sought feedback on topics related to future directions for NIST and the NCCoE’s work in this important space. With the release of EO 14028, the Cybersecurity for IoT Program was engaged in the requirements to develop cybersecurity criteria for consumer IoT as a part of the greater NIST EO response effort. Work started before the EO with a white paper, "*Establishing Confidence in IoT Device Security: How do we get there?"*, which explored the various dimensions of confidence mechanisms that could be applied and assessed available alternative approaches for providing confidence in the cybersecurity of IoT devices. This helped define an available landscape of approaches to consider in developing guidance for consumer IoT. These insights helped to inform EO 14028 response efforts, leading up to the draft Baseline Security Criteria for Consumer IoT Devices, which was published in August 2021 and discussed in a public workshop the following month.

To provide IoT cybersecurity guidance for federal agencies, NIST also published other public review drafts early in FY 2021:

- *IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements* (draft NIST SP 800-213) and
- *Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government* (draft NISTIR 8259D).

These drafts were released concurrently with the signing of the IoT Cybersecurity Improvement Act of 2020. Work to refine the information from these drafts continued through FY 2021, using many of the same stakeholder engagement activities that supported the development of NISTIR 8259B, and the program anticipates publishing final versions of its guidance for federal agencies early in FY 2022.

Throughout this period, the Cybersecurity for IoT Program has remained engaged with international activities. In particular, program representatives have been active in the progress of *Cybersecurity — IoT security and privacy — Device baseline requirements*, ISO/IEC 27402.

Open Security Controls Assessment Language (OSCAL)

As systems become more complex and more cloud solutions are adopted, the responsibilities of security practitioners and authorizing officials are increasingly difficult. They must employ multiple sets of documents while leveraging a thorough understanding of systems’ interconnections and dependencies, and how controls are inherited from other systems to better mitigate risks.

In July 2021, NIST released the Open Security Controls Assessment Language (OSCAL) 1.0.0, to support interoperable and portable security automation. OSCAL applies security documentation as code (i.e., documentation in machine-readable formats) for integration into security assessment, auditing, and monitoring activities. Through this model, OSCAL provides traceability throughout the risk management process, including automation of authorization to operate (ATO) tasks.

OSCAL, developed through a community-centric approach, is an open source set of formats. NIST encourages all interested parties to join the community and support the improvement and expansion of OSCAL. Adoption of OSCAL is expanding, including the NIST SP 800-53 security and privacy controls SP 800-53A assessment procedures, and GSA FedRAMP’s SP 800-53 security baselines. International adoptions include the European Union Agency for Cybersecurity (ENISA) use of OSCAL for the automation of their conformity assessment process for this program and the ISO/IEC Subcommittee 27 (SC27) Working Group 1 (WG1) approval to release the 27002:2022 standard in OSCAL.

Artificial Intelligence (AI)

NIST contributes to the research, standards, evaluation, and data required to advance the development, use, and governance of trustworthy AI. NIST aims to cultivate trust in the design, development, and use of AI technologies and systems by improving measurement science, technology, standards, and related tools in ways that enhance economic security and improve quality of life.

AI and Machine Learning (ML) are already changing the ways in which society addresses economic and national security challenges and opportunities, and these technologies must be developed and used in a trustworthy and responsible manner. Characteristics that support trustworthiness include accuracy, explainability, interpretability, reliability, privacy, robustness, safety, security (resilience), and the mitigation of harmful bias. Principles such as transparency, fairness, and accountability should be considered, especially during deployment and use. Many of these characteristics and principles are described in the work and publications at NIST ITL's Artificial Intelligence site.

Trustworthy data, standards, evaluation, validation, and verification are critical for the successful deployment of new technologies for genomics, image and video processing, materials, natural language processing, robotics, wireless spectrum monitoring, and more.

Delivering the needed measurements, standards, and other tools is a primary focus of NIST's portfolio of AI efforts. It is an area in which NIST has special responsibilities and expertise and for which others often turn to NIST for guidance. NIST's AI goals and activities are prioritized and informed by its statutory mandates, White House directives, and the needs expressed by industry, other federal agencies, and the global AI research community.

NIST's continued AI work is aligned with five broad goals:

1. Conduct fundamental research to advance trustworthy AI technologies.
2. Apply AI research and innovation across the NIST Laboratory Programs.
3. Establish benchmarks and develop data and metrics to evaluate AI technologies.
4. Lead and participate in the development of technical AI standards.
5. Contribute to discussions and the development of AI policies.

The NCCoE, in collaboration with industry and academic partners, has developed Dioptra, an experimentation testbed to address the broader challenge of the evaluation of ML algorithms' defenses and their resistance to attack. The testbed aims to facilitate security evaluations of ML algorithms under a diverse set of conditions. The testbed has a modular design that enables researchers to easily substitute alternative datasets, models, attacks, and defenses. The result is the ability to advance the metrology needed to help secure ML-enabled systems. NIST is expanding the user base for Dioptra and developing additional capabilities.

NIST has also initiated projects to address cybersecurity challenges in AI-enabled healthcare and semi-autonomous vehicles. The outcome of these efforts will be to provide practical guidance on addressing these challenges. NIST will continue to collaborate with commercial, academic, and public-sector partners to pursue these goals and collectively advance the security and trustworthiness of this important and emerging technology.

7 | Trustworthy Networks

Credit: Shutterstock

NIST's Trustworthy Networks Program works with industry partners to advance the research, standardization, and adoption of the technologies that are necessary to increase the security, privacy, robustness, and performance of networked systems. This includes resolving systemic vulnerabilities in existing and emerging critical network infrastructures and advancing the development of potentially disruptive technologies to improve the trustworthiness of future networks. To achieve these goals, NIST works closely with standards development organizations to improve the quality and timeliness of emerging technical specifications. NIST's contributions often include innovating and applying the measurement science necessary to improve an industry's trust and confidence in the design and deployment of new technologies. NIST's contributions follow the full cycle of problem identification, standardization of solutions, development of reference implementations and test tools, publication of deployment guidance, and demonstration and documentation of the recommended practices when using the resulting commercial products and services.

Core Network Infrastructure Resilience

The following sections describe NIST's focus on current and emerging technologies that underlie almost all communication and information systems, spanning enterprise, Internet, and consumer networks.

Internet Infrastructure Protection

Addressing systemic vulnerabilities in the Internet's foundational protocols and infrastructure has been identified as a national priority. NIST's Internet Infrastructure Protection efforts aim to expedite the design, standardization, commercialization, and deployment of new technologies to address systemic vulnerabilities in the core infrastructure of the modern Internet. NIST has a long history of working with the Internet industry to standardize and promulgate new technologies to address pressing security and robustness issues in core Internet protocols.

In FY 2021, the Robust Inter Domain Routing project developed the NIST RPKI (Resource Public Key Infrastructure) Monitor – a test and measurement system designed to monitor Internet routing dynamics. Its purpose is to provide measurement data and analyses to research, standardization, and operations communities to improve the trust and confidence in the underlying Internet security technologies.

NIST's contributions to expedite the design, standardization and adoption of technologies to dramatically improve the security and resilience of the Internet's routing infrastructure are widely recognized. Numerous major enterprises and service providers use NIST's test and measurement tools, reference implementations, and deployment guidance. NIST's leadership, based on beneficial impacts in this area, was awarded a Department of Commerce Gold Medal in 2021.

Transition to IPv6-Only Networks

In November 2020, OMB published *Completing the Transition to Internet Protocol Version 6 (IPv6)*, Memorandum M-21-07, setting milestones for the Federal Government to deliver its information services, operate its networks, and access the services of others using only IPv6. This U.S. Government (USG) implementation of IPv6 is frequently referenced as USGv6. This memorandum tasked NIST with two key roles: (1) updating the USGv6 standards profiles and test program to facilitate USG acquisition of secure and interoperable IPv6 products and services and (2) leading an NCCoE demonstration pilot focused on the secure deployment of IPv6-only networks within the enterprise.

In response to this tasking, in FY 2021, NIST published a significant revision to the USGv6 Profile and Test Program to incorporate the latest advances in Internet Engineering Task Force (IETF) standards, security requirements, and practice guides. Enhancements to the USGv6 product testing framework provide the conformance, interoperability, and functional testing necessary to foster trust and confidence in the deployment of IPv6 products in mission-critical government networks. NIST also initiated work on a new NCCoE project focused on Secure IPv6-Only Implementation in the Enterprise. In this effort, NIST will collaborate with industry partners to demonstrate the commercial viability of and document recommended practices for the secure evolution of government enterprise networks to meet the new OMB IPv6-only requirements.

Zero Trust Networks

A transition to a "zero trust" approach to security provides a defensible architecture. As described in the Department of Defense Zero Trust Reference Architecture, "The foundational tenet of the Zero Trust Model is that no actor, system, network, or service operating outside or within the security perimeter is trusted. Instead, we must verify anything and everything attempting to establish access. It is a dramatic paradigm shift in philosophy of how we secure our infrastructure, networks, and data, from verify once at the perimeter to continual verification of each user, device, application, and transaction."

In FY 2021, the NCCoE, in collaboration with industry participants, initiated a project to demonstrate several approaches to a zero trust architecture applied to a conventional, general-purpose enterprise IT infrastructure on-premises and in the cloud, which will be designed and deployed according to the concepts and tenets documented in *Zero Trust Architecture* (SP 800-207). Over 20 companies have joined the collaborative effort to demonstrate the application of zero trust technologies to modern enterprise IT environments. The example implementations will integrate commercial and open-source products that leverage cybersecurity standards and recommended practices to showcase the robust security features of zero trust architectures. This project will result in a NIST Cybersecurity Practice Guide – a publicly available description of the practical steps needed to implement the cybersecurity reference designs for zero trust and a logical architecture of a general Zero Trust Architecture (ZTA) reference design (see Figure 1).

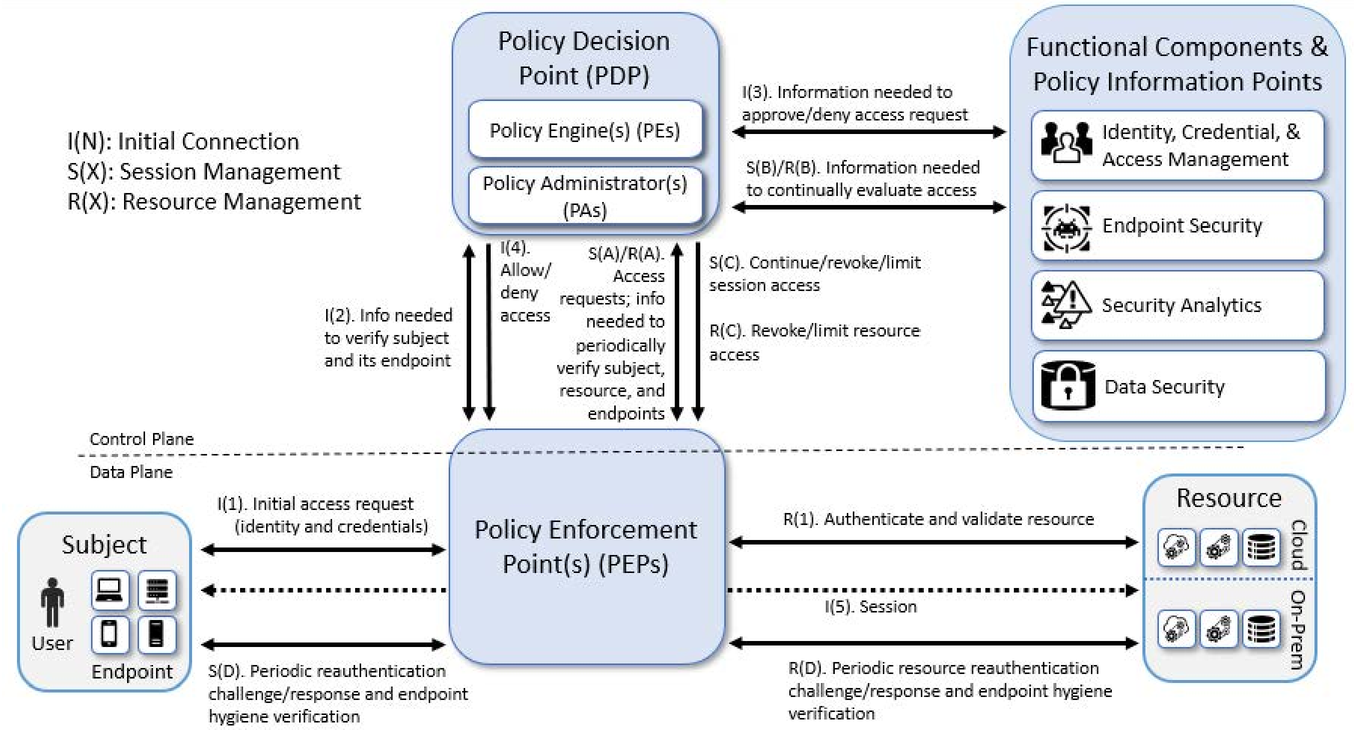

I(N): Initial Connection
S(X): Session Management
R(X): Resource Management
Policy Decision Point (PDP)
Policy Engine(s) (PEs)
Policy Administrator(s) (PAs)
I(3). Information needed to approve/deny access request
S(B)/R(B). Information needed to continually evaluate access
Functional Components & Policy Information Points
Identity, Credential, & Access Management
Endpoint Security
Security Analytics
Data Security
I(2). Info needed to verify subject and its endpoint
I(4). Allow/ deny access
S(A)/R(A). Access requests; info needed to periodically verify subject, resource, and endpoints
S(C). Continue/revoke/limit session access
R(C). Revoke/limit resource access
Control Plane
Data Plane
I(1). Initial access request (identity and credentials)
Policy Enforcement Point(s) (PEPs)
R(1). Authenticate and validate resource
I(5). Session
Subject
User
Endpoint
Resource
Cloud
On-Prem
S(D). Periodic reauthentication challenge/response and endpoint hygiene verification
R(D). Periodic resource reauthentication challenge/response and endpoint hygiene verification

Figure 1: Components of a Zero Trust Architecture

Security for 5G and Subsequent Generations

In October 2021, the NCCoE began a project focused on the technical aspects of cybersecurity for 5G (fifth-generation technology standard for broadband cellular networks). 5G refers to a recent generation of wireless communications systems, which are faster and carry more data than previous generations. The NCCoE project is a collaboration of 12 industry-leading organizations that are contributing hardware and software valued at over $1 million. The expected outcome of the project is an example 5G implementation that provides a holistic approach to 5G cybersecurity, focusing on both standards-defined cybersecurity features as well as cloud technologies that can provide foundational cybersecurity features outside of the scope of the existing 5G security architecture. The resulting security reference architecture for 5G networks will bridge the gap between IT and telecommunications cybersecurity. In FY 2021, the collaboration published a draft executive summary (SP 1800-33A) for the project while successfully designing, planning, and beginning the deployment of the commercial-grade 5G technology components.

The project continued the deployment of the 5G network testbed with the goal of getting the first 5G call early in calendar year 2022. The project will publish a preliminary draft of a practice guide (SP 1800-33B) that highlights all of the cybersecurity capabilities offered by a 5G system and enabled by the project's reference architecture.

Security of Domain-Specific Networks

This section describes research and projects that focus on the unique requirements and risks found in specific use cases and unique application domains.

IoT Network Security

NIST's efforts to advance the design, standardization, commercialization, and adoption of new technologies to improve the security and resilience of the emerging Internet of Things has focused its recent efforts on consumer and enterprise network environments. In FY 2021, NIST completed several projects focused on emerging Manufacturer Usage Description (MUD) technologies, including the development of an open-source, pure software-defined network (SDN) implementation of a MUD manager and policy enforcement points, methodologies, and tools to automate the generation of MUD profiles for IoT devices, as well as NCCoE practice guides for Securing Home IoT Devices Using MUD.

NIST's ongoing work in emerging IoT security technology is focused on advancing the development of trusted IoT device on-boarding and life cycle management. NIST developed a white paper and conducted a workshop to help focus attention on this problem space and emerging solutions. NIST initiated a new NCCoE demonstration project to develop practice guides for secure IoT device on-boarding and life cycle management.

Industrial and Operational Technology Networks

In FY 2021, the NCCoE collaborated with engineers from NIST's Engineering Lab to improve the security and resilience of industrial and operational technology networks that span multiple application domains, including general industrial control systems and manufacturing environments. Members of the Protecting Information and System Integrity in Industrial Control System Environments project published a draft practice guide, *Cybersecurity for the Manufacturing Sector* (draft SP 1800-10). Manufacturers, and their increasingly interconnected operational technology (OT) and information technology (IT) systems, have become major targets of cybersecurity attacks. The goal of the project was to demonstrate example solutions that manufacturers can use to protect their systems from destructive malware, insider threats, advanced persistent threats, and unlicensed software. Technology providers and industry experts, including several National Cybersecurity Excellence Partnership (NCEP) collaborators, contributed to example solutions that were implemented in two distinct but related labs, each with two settings: robotics-based manufacturing and process control systems that resemble what is being used by chemical manufacturing industries.

NIST initiated an update of the *Guide to Industrial Control Systems (ICS) Security* (SP 800-82) to incorporate lessons learned over the past several years, to provide alignment to relevant NIST guidance and other control system cybersecurity standards and recommended practices, and to address changes in the threat landscape. A pre-draft call for comments was initiated in April 2021, and the initial public draft of SP 800-82, Rev. 3 is currently scheduled for FY 2022. Updates include expanding the scope from ICS to control systems/OT, applying new cybersecurity capabilities, adding guidance specific to small- and medium-sized control system/OT owners and operators, and revising information about relevant threats, vulnerabilities, standards, and recommended practices.

In FY 2021, the NIST Smart Grid Program published guidance documents and a mapping tool for improving cybersecurity in power systems. The fourth revision of NIST's Smart Grid Interoperability Framework described complementary approaches to ensuring cybersecurity: one based on assessing and mitigating organizational risk by applying concepts from NIST's Framework for Improving Critical Infrastructure Cybersecurity to utility organizations and the second based on examining the specific logical interfaces introduced through distributed energy resources to characterize the cybersecurity requirements necessary to explore individual assets. This provided guidance has become a foundation for cybersecurity training offered by the National Association of Regulatory Utility Commissioners to government officials, as well as technical working groups in industry organizations.

NIST also collaborated in the development of a mapping tool and an associated guidance document that clarify the relationship between the cybersecurity outcomes and best practices described in the NIST Cybersecurity Framework and the latest version of the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards. This mapping is critical to the industry, as NERC CIP standards are the enforceable cybersecurity standards for the grid, and the relationship between NERC CIP and NIST cybersecurity best practices is not always clear.

Network Security Research

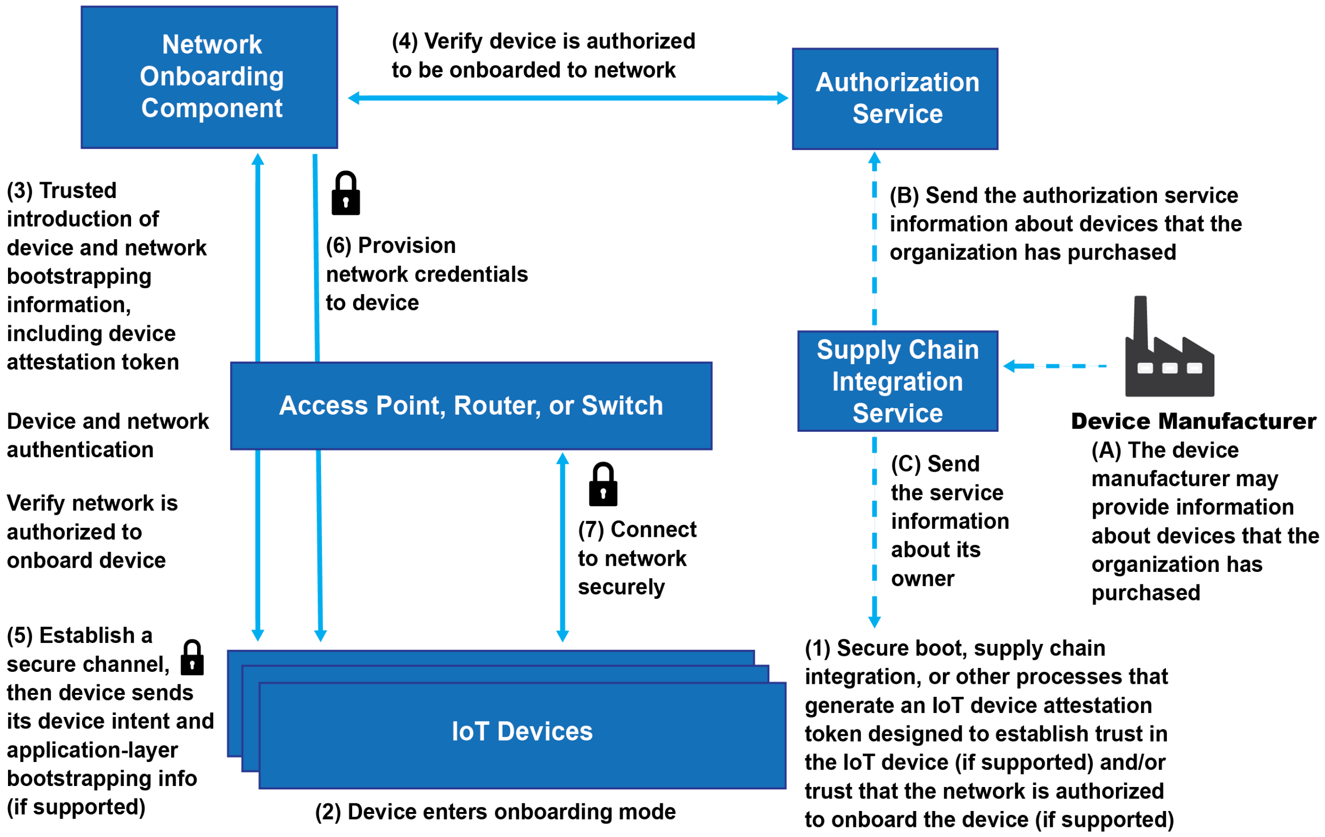
This third topic area looks beyond the horizon of current and emerging networks to address the security and resilience challenges of future networks by exploring potentially disruptive technologies.

AI Applications to Network Security

In FY 2021, NIST's Trustworthy Intelligent Networks project researched the application of AI techniques to detect malicious botnet traffic in both data centers and the public internet. Botnets and their ability to launch large-scale, distributed denial-of-service (DDoS) attacks remain a serious threat to all forms of networked critical infrastructure. NIST developed deep learning techniques to detect botnet command and control channels that exploit the domain name system (DNS). NIST researched advanced state-of-the-art algorithms to detect botnet abuse through domain-generation algorithms in the DNS.

Formal Verification of Security Protocols

The complexity and pace of innovation of new network security protocols in numerous realms challenge industries' ability to conduct careful reviews of their designs. To address that challenge, NIST is exploring the use of formal methods to verify the security properties of protocol designs early in their standardization process. NIST's Trustworthy Internet of Things project is one such effort that explores the application of formal methods to verify the security properties of emerging IoT on-boarding technologies (see Figure 2). In FY 2021, NIST published research on the automated formal verification of Bootstrapping Remote Secure Key Infrastructures (BRSKI) protocol. Ongoing efforts are exploring additional formal verification methods and their applications to an expanded scope of emerging designs for IoT on-boarding protocols.



Network Onboarding Component
(4) Verify device is authorized to be onboarded to network
Authorization Service
(3) Trusted introduction of device and network bootstrapping information, including device attestation token
(6) Provision network credentials to device
(B) Send the authorization service information about devices that the organization has purchased
Supply Chain Integration Service
Device Manufacturer
(A) The device manufacturer may provide information about devices that the organization has purchased
Access Point, Router, or Switch
Device and network authentication
Verify network is authorized to onboard device
(7) Connect to network securely
(C) Send the service information about its owner
(5) Establish a secure channel, then device sends its device intent and application-layer bootstrapping info (if supported)
IoT Devices
(1) Secure boot, supply chain integration, or other processes that generate an IoT device attestation token designed to establish trust in the IoT device (if supported) and/or trust that the network is authorized to onboard the device (if supported)
(2) Device enters onboarding mode

Figure 2: Functional Diagram of IoT Onboarding Protocols

8 | Trustworthy Platforms

Credit: Shutterstock

NIST defines a platform as a computer or hardware device, operating system, or virtual environment on which software can be installed or run. The goal of the Trustworthy Platforms focus area is to improve trust in the security and privacy of these systems and infrastructures by providing guidance and technologies for the development and use of secure platforms, including software, hardware, and firmware. A trustworthy platform is a dynamic ecosystem that depends on multiple security and privacy technologies for reliable service delivery. It is deployed and maintained in a measured state that is known to protect the security and privacy of users and data, and it performs services in a consistent and reliable manner. The desired outcome of the NIST focus area is to increase the adoption of trustworthy platforms in order to improve trust in the security and privacy of systems and infrastructures. NIST provides guidance and technologies for the development and use of secure platforms and foundational components such as cryptography. NIST also helps to develop quantifiable measurements that provide assurances for platform security, privacy, and robustness.

Enhancing the Security of the Software Supply Chain – Implementation of EO 14028

The President's Executive Order (EO) 14028, Improving the Nation's Cybersecurity, issued on May 12, 2021, charged multiple agencies – including NIST – with enhancing cybersecurity through a variety of initiatives related to the security and integrity of the software supply chain. In support of EO 14028, NIST solicited position papers and other input from the community, hosted a series of workshops, and consulted with other federal agencies. NIST published a definition of "critical software" within the context of EO 14028, guidance that outlines security measures for critical software use, and recommended minimum standards for vendor or developer verification of software. NIST has also published *Cyber Supply Chain Risk Management Practices for Systems and Organizations* (draft SP 800-161, Revision 1) and *Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities* (SP 800-218). Work in support of EO 14028 will continue throughout FY 2022.

Secure Software Development Framework (SSDF)

The Secure Software Development Framework (SSDF) is a set of fundamental secure software development practices based on established practice documents from organizations such as BSA, OWASP, and SAFECode. Few software development life cycle (SDLC) models explicitly address software security in detail, so practices like those in the SSDF need to be added to and integrated with each SDLC implementation.

Following the SSDF practices should help software producers reduce the number of vulnerabilities in released software, mitigate the potential impacts of the exploitation of undetected or unaddressed vulnerabilities, and address the root causes of vulnerabilities to prevent future recurrences. Because the SSDF provides a common vocabulary for secure software development, software consumers can also use it to foster communications with suppliers in acquisition processes and other management activities.

In September 2021, NIST released *Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities* (draft SP 800-218). SP 800-218 will replace the NIST Cybersecurity White Paper released in April 2020, which defined the original SSDF. Changes from version 1.0 to 1.1 include adding several references, creating new practices and tasks related to secure software development environments, and mapping SSDF practices to corresponding clauses from EO 14028.

NIST will continue to refresh and evolve the SSDF in response to public feedback and the changing threats, vulnerabilities, practices, and automation capabilities in software development. Future work may potentially cover topics such as how the SSDF may apply to and vary for particular software development methodologies and associated practices like DevOps and how an organization can transition from using just their current software development practices to also incorporating the practices specified by the SSDF.

Improving Cybersecurity in Supply Chains

In August 2021, NIST launched the National Initiative for Improving Cybersecurity in Supply Chains to help organizations build, evaluate, and assess the cybersecurity of products and services in their supply chains, an area of increasing concern. The effort will emphasize tools, technologies, and guidance focused on the developers and providers of technology. At the same time, there is a need among those acquiring products and services for cohesive, practical, performance-oriented guidance to address the broader cybersecurity risks to the security and resilience of all supply chains. NIST expects to issue a Request for Information in FY 2022 to help guide this public-private partnership.

Hardware-Enabled Security

The foundation of any data center or edge computing security strategy should be securing the platform on which data and workloads will be executed and accessed. The physical platform represents the first layer for any layered security approach and provides the initial protections to help ensure that higher-layer security controls can be trusted. In FY 2021, the NCCoE continued to develop and demonstrate approaches based on hardware-enabled security techniques and technologies for safeguarding data and workloads. *Hardware-Enabled Security: Container Platform Security Prototype* (NISTIR 8320A) was finalized in June 2021, and a second public comment draft of *Hardware-Enabled Security: Enabling a Layered Approach to Platform Security for Cloud and Edge Computing Use Cases* (NISTIR 8320) was released in May 2021. Additional publications in the NISTIR 8320 series are also under development.

Control System and Operational Technology (OT) Security

NIST is incorporating lessons learned in revisions to the *Guide to Industrial Control Systems (ICS) Security* (SP 800-82) (see previous section) to provide alignment to relevant NIST guidance (e.g., SP 800-37, Rev. 2; SP 800-53, Rev. 5; SP 800-53B; and Cybersecurity Framework v1.1) and other relevant control system cybersecurity standards and recommended practices, and address changes in the threat landscape. Updates include expanding the scope from ICS to control systems/OT, applying new cybersecurity capabilities, adding guidance specific to small and medium-sized control system/OT owners and operators, and revising the control system/OT threats, vulnerabilities, standards, and recommended practices.

Ransomware and Data Security

The term “ransomware” describes types of malware used by perpetrators to carry out threats to publish a victim’s sensitive personal or business information or to perpetually block the victim’s access to vital information unless a ransom is paid. Ransomware attacks can paralyze or destroy organizations. NIST undertook several activities (see below) to help organizations protect against ransomware attacks and to enable recovery from any that are successful.

Ransomware protection and remediation require a coordinated response involving processes, procedures, and decision-making using technical controls for identifying, mitigating, and recovering from ransomware events. To help organizations access the NIST guidance and tools that best address these needs, NIST’s new Ransomware Protection and Response page aggregates NIST recommendations that directly address the ransomware challenge. The page includes a "tips and tactics" one-pager providing key actions for defense against ransomware attacks. To support small and medium-sized organizations, the Small Business Cybersecurity Corner now features a ransomware page that illustrates ransomware event basics, how ransomware events can impact businesses of all sizes, and actions that can help in managing ransomware risk.

In response to several major recent ransomware events, NIST also engaged industry experts in drafting a new *Cybersecurity Framework Profile for Ransomware Risk Management* publication (draft NISTIR 8374). This profile identifies relevant subcategories and informative references from the NIST Cybersecurity Framework and maps them directly to ransomware risk management activities. Additionally, the document includes a high-level description of security measures that organizations can take now to prevent future ransomware attacks and mitigate the consequences of any successful attacks.

Complementing the new ransomware profile, the NCCoE published two practice guides: *Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events* (SP 1800-25) and *Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events* (SP 1800-26). These publications are a continuation of the previously published *Data Integrity: Recovering from Ransomware and Other Destructive Events* (SP 1800-11). Together, the practice guides demonstrate how commercially available technology can be used to implement the Cybersecurity Framework. These NCCoE SPs are supplemented by NIST’s *Securing Data Integrity Against Ransomware Attacks* (draft NIST CSWP 10012020) white paper that was published to help organizations apply the architectures described in the practice guides to preventing or mitigating ransomware events. These are supported by the Ransomware Protection and Response web page described above.

Distributed Energy Resource (DER) Security

In FY 2021, NIST's NCCoE Energy Sector team completed the project started in FY 2020 on protecting Industrial Internet of Things (IIoT) devices at the grid edge (the components that extend the traditional power grid infrastructure and that include physical assets [e.g., smart meters], applications, and data analytics tools). The team investigates data integrity concerns that arise from the use of distributed energy resources (DERs), such as photovoltaics. The team developed an associated draft practice guide, *Securing the Industrial Internet of Things: Cybersecurity for Distributed Energy Resources* (SP 1800-32). The practice guide addresses a key challenge for all energy operators and owners: protecting the integrity of the data needed to execute command and control to maintain the resilience of the grid.

NIST participated in and provided contributions to the IEEE (Institute of Electrical and Electronics Engineers) 1547.3 working group in their effort to develop a Guide for Cybersecurity of Distributed Energy Resources (DER) Interconnected with Electric Power Systems. The document provides cybersecurity guidelines for DER stakeholders, including utilities, aggregators, and DER vendors, owners, and operators. NIST also organized a Smart Electric Power Alliance (SEPA) half-day workshop in March 2021 to understand the usage of the cybersecurity controls for the logical interface categories defined in *Guidelines for Smart Grid Cybersecurity* (NISTIR 7628) by DER stakeholders. The workshop results and conclusions will be used to inform future SEPA and NIST efforts.

Systems Security Engineering

The NIST Systems Security Engineering Project initiated major updates to its publications. *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach* (SP 800-160, Volume 2, Revision 1) helps organizations anticipate, withstand, recover from, and adapt to adverse conditions, stresses, or compromises on systems, including hostile and increasingly destructive attacks from nation-states, criminal gangs, and disgruntled individuals. This update offers significant new content and support tools for organizations to defend against attacks. The document provides suggestions on how to limit the damage that adversaries can inflict by impeding their lateral movement, increasing their work factor, and reducing their time on target. The update also adds an appendix analyzing the potential effects of cyber resiliency on adversary tactics, techniques, and procedures used to attack OT systems.

NIST also continued its update to *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems* (SP 800-160, Volume 1, Revision 1). Content was added to help organizations develop systems that are "secure by design" with an emphasis on the use of design principles for trustworthy, secure systems. The guideline is also being updated to ensure consistency with international systems and software engineering standards.

Leadership and Participation in National and International Standards Programs

Credit: Shutterstock

During FY 2021, NIST staff contributed to and held leadership positions in various standards developing organizations (SDOs), including the International Electrotechnical Commission (IEC), the Internet Engineering Task Force (IETF), the Institute of Electrical and Electronics Engineers (IEEE), the World Wide Web Consortium (W3C), the 3rd Generation Partnership Project (3GPP), and the International Organization for Standardization (ISO). NIST also supports ANSI (American National Standards Institute) X9, a non-profit standards development organization chartered to develop voluntary open consensus standards for the financial services industry in the US. The staff actively participated in standards bodies to raise awareness and influence the development of privacy and cybersecurity standards, including efforts within the ISO/IEC (Joint Technical Committee - JTC1).

NIST uses collaborative opportunities to highlight the role that standards play in enabling technological innovation and interoperability among products and systems. International collaboration and alignment on standards-based approaches to cybersecurity and privacy risk management lead to greater innovation and a more effective and efficient utilization of resources. NIST also shares information on standards processes, the importance of standards on the economy and facilitating international trade, and the ability of standards to help secure systems and infrastructure. NIST coordinates with interagency partners on strategic approaches and communication on standards for the Federal Government.

The standards community is built upon international collaboration, and NIST leverages its foundational and applied research efforts and experience in leadership to contribute to the development of national and international standards. These standards activities span cybersecurity, privacy, cryptography, Identity Management, and critical fields, such as 5G mobile and cellular technologies, quantum technologies, cloud infrastructure management, blockchain and distributed ledger technologies, the Internet of Things (IoT), vehicle automation, and artificial intelligence (AI).

In FY 2021, NIST continued to engage with government and industry organizations to demonstrate and ensure continued alignment with voluntary international standards. NIST discussed the Cybersecurity Framework in numerous dialogues and has continued to identify and promote international adaptations and translations of the Framework, which is now available in 10 languages. NIST also continues to contribute to international standards development efforts related to cybersecurity risk management and the development of cybersecurity frameworks, including Cybersecurity framework guidelines, ISO/IEC Technical Specification 27110, which was published in February 2021.

NIST has been instrumental in promoting and participating in the development of a family of voluntary ISO/IEC standards that align with NIST's cryptographic module validation standard and related specifications. NIST served as the project editor for nine of those standards.

Other significant examples of NIST staff engagement in the standards space include the mobile driver license project (ISO/IEC 18013-5); work on draft ISO/IEC 23894, Artificial Intelligence Risk Management; a leadership position for the work on Trusted Execution Environments in the IETF; and contributions to Zero Trust Protocols and Quantum Computing in the ISO committee for Cryptography (ISO IEC JTC1/SC27/WG2).

About 100 NIST staff members work with other agencies and industry leaders to develop cybersecurity and privacy standards through voluntary consensus. NIST's standards strategy is captured in *Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity* (NISTIR 8074).

In FY 2022, the NIST staff will continue to lead and participate in cybersecurity and privacy standardization efforts with an increased focus on new and emerging areas, such as quantum information, 5G communications, and zero trust architectures.

Opportunities to Engage with the NIST Cybersecurity & Privacy Program

Credit: Shutterstock

Collaborators and researchers are an important force behind NIST's cybersecurity and privacy programs. NIST depends on developers, providers, and everyday users of cybersecurity and privacy technologies and information to guide priorities in serving the public and private sectors. These stakeholders are also vital when it comes to decisions about the best methods and formats for delivering information and services.

NIST engages in the public and private sectors in many ways, both formal and informal. NIST participates in various forums, communities of interest (COI), joint research efforts, standards development organizations, student programs, and other partnership opportunities that are available; hosts/sponsors various cybersecurity and privacy events; and gathers public feedback on NIST publications, blogs, and social media.

Further details on engaging with NIST on Cybersecurity and Privacy are available at https://www.nist.gov/cybersecurity/cybersecurity-privacy-stakeholder-engagement.

Guest Researcher Opportunities at NIST

Many NIST projects are supported by guest researchers, both foreign and domestic. The Domestic Guest Researcher (DGR) Program provides access for technically qualified U.S. citizens to NIST facilities and equipment while working with the NIST staff on projects of mutual interest. The Foreign Guest Researcher Program offers scientists from around the world the opportunity to work collaboratively with NIST scientists. Guest researcher support generally comes from sponsoring companies or organizations, including the home organizations of the researchers.

The Pathways Program offers clear paths to federal internships for students from high school through post-graduate school and to careers for recent graduates, as well as meaningful training and career development opportunities for individuals who are at the beginning of their federal service.

Funding Opportunities at NIST

NIST funds industrial and academic research in several ways. The Small Business Innovation Research Program funds research and development (R&D) proposals from small businesses. NIST offers grants to encourage work in the fields of precision measurement, fire research, and materials science. Grants and awards supporting research by industry, academia, and other institutions are also available on a competitive basis through various NIST offices.

For general information on the NIST grants programs, please contact Mr. Christopher Hunton at (301) 975-5718 or by email at grants@nist.gov.

AUTHORITY

This publication has been developed by the National Institute of Standards and Technology (NIST) in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3541. Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would be appreciated by NIST.

HOW TO CITE THIS NIST TECHNICAL SERIES PUBLICATION

O'Reilly PD, II, Rigopoulos KG, Feldman L, Witte GA (2022) Fiscal Year 2021 Cybersecurity and Privacy Annual Report. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-220. https://doi.org/10.6028/NIST.SP.800-220

DISCLAIMER

Any mention of commercial products or organizations is for informational purposes only; it is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the products identified are necessarily the best available for the purpose.

ACKNOWLEDGMENTS

The editors would like to thank their NIST colleagues who provided write-ups on their project highlights and accomplishments for this annual report. They appreciate the work of Elaine Barker, Sara Kerman, Jeff Marron, and Isabel Van Wyk for reviewing and providing valuable feedback for this annual report.

TRADEMARK INFORMATION

All names are trademarks or registered trademarks of their respective owners.

BACKGROUND INFORMATION OF ANNUAL REPORT

This Annual Report provides the opportunity to describe the many cybersecurity program highlights and accomplishments from throughout the NIST Information Technology Laboratory (ITL). The report is organized into several focus areas that highlight key research topics and highlights. ITL, an operating unit under NIST, contains seven divisions. Cybersecurity work is conducted by each division, and it is the sole focus for the Applied Cybersecurity and Computer Security Divisions. Throughout this Annual Report, there are references to particular division activities, and often to work by groups within those divisions.

Please note: This Annual Report covers the Federal Government's Fiscal Year (FY) 2021, from October 1, 2020 to September 30, 2021.

ABSTRACT

During Fiscal Year 2021 (FY 2021) – from October 1, 2020, through September 30, 2021 – the NIST Information Technology Laboratory (ITL) Cybersecurity and Privacy Program successfully responded to numerous challenges and opportunities in security and privacy. This annual report highlights the FY 2021 research agenda and activities for the ITL Cybersecurity and Privacy Program, including the ongoing participation and development of international standards; the enhancement of privacy and security risk management models, including those for the protection of controlled unclassified information (CUI), systems engineering and cyber resiliency, supply chains, and mobile technologies; the continued advancement of cryptographic technologies, including updates to Federal Information Processing Standard (FIPS) Publication 140-3, Security Requirements for Cryptographic Modules, and preparation for post-quantum cryptographic methods; and improved infrastructure protection in areas such as zero trust architectures and advanced networking security. NIST maintained a strong focus on supporting small and medium-sized businesses (SMBs), including updates to the Small Business Cybersecurity Corner website to make resources easier to find and use and drawing on contributed cybersecurity resources and feedback received from federal partners and the public.

KEYWORDS

annual report; cybersecurity; Federal Information Security Management Act; FISMA; privacy; program highlights; information security; Information Technology Laboratory; ITL.

REPORTS ON COMPUTER SYSTEMS TECHNOLOGY

The Information Technology Laboratory (ITL) at NIST promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

NATIONAL INSTITUTE OF
STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE