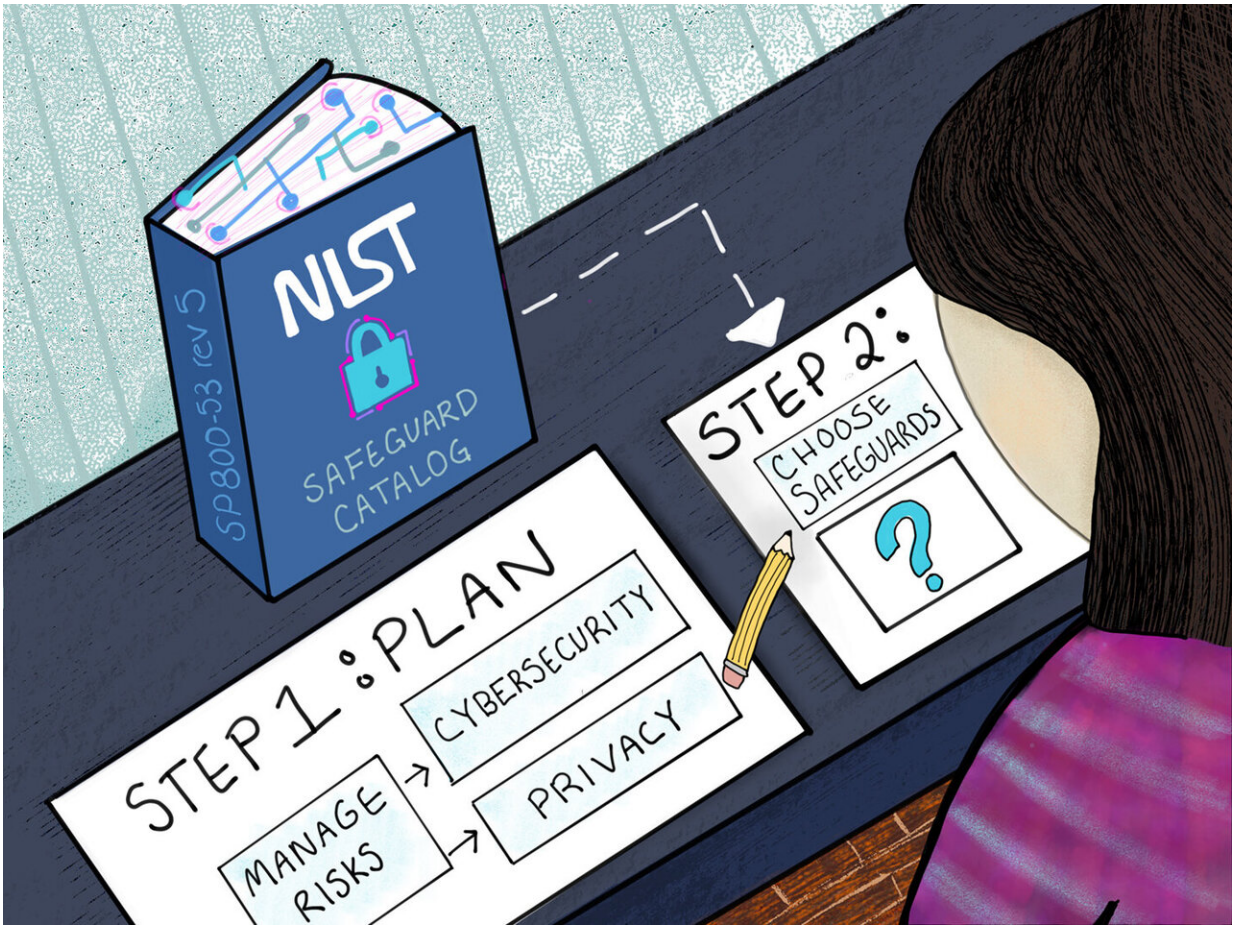
NIST updates and expands its flagship catalog of information system safeguards

March 17 2020



After forming a general plan for tackling your cybersecurity and privacy risk management issues, you need state-of-the-art tools to make that plan a reality. Find them in NIST's updated catalog. Credit: N. Hanacek/NIST

After your organization forms a general plan for tackling its cybersecurity and privacy risk management issues, it needs particular state-of-the-art tools to make that plan a reality. Computer security and privacy experts at the National Institute of Standards and Technology (NIST) have the answer with an updated toolbox of safeguards for protecting an organization's operations and assets, as well as the personal privacy of individuals.

NIST Draft Special Publication (SP) 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations, is a collection of hundreds of specific measures for strengthening the systems, component products and services that underlie the nation's businesses, government and critical infrastructure. One of NIST's flagship risk management publications, the document is undergoing its first update in seven years, and the agency is accepting public comments on the draft until May 15, 2020.

The publication offers safeguards for all types of platforms, from general-purpose computers to industrial control systems and internet of things (IoT) devices. Its tools are intended for a broad audience of specialists, from security experts to systems developers to cloud computing providers.

"Our objective is to make the information systems we depend on more resistant to cyberattacks," said NIST's Ron Ross, one of the publication's authors. "We want to limit the damage from those attacks when they occur, make the systems cyber-resilient, and at the same time protect the security and privacy of information."

The safeguards, or "controls" as they are called in the title, come in different forms, from technical solutions (like encryption) to operational strategies (like plans for cyberattack incident response) to management approaches (like conducting a risk assessment). Altogether, the

publication organizes hundreds of controls into 20 related groups.

The use of these controls is mandatory in federal information systems, but the controls can be selectively tailored and implemented within any organization. Along with other supporting NIST publications, the catalog is designed to help federal organizations identify the controls needed to satisfy the security and privacy requirements in the Federal Information Security Management Act (FISMA), the Privacy Act of 1974, Office of Management and Budget policies and certain Federal Information Processing Standards (FIPS).

How can an organization incorporate this catalog into its broader effort to increase security and privacy? Ross said that the first step is to assess the risks confronting an organization using tools such as NIST's Risk Management Framework, Cybersecurity Framework and Privacy Framework. Through the use of these frameworks, the organization can identify where it needs safeguards, and then it can turn to the catalog to find specific solutions.

"An organization can use this catalog together with any approach to risk management," Ross said. "We reference other NIST publications for readers' convenience, but we have designed it to be agnostic."

The fifth revision contains a number of improvements over SP 800-53's previous versions:

- A complete integration of privacy into the controls. Whereas in earlier editions, privacy was consigned to an appendix, here the controls are part of the unified catalog, which should make life easier for users of the NIST Privacy Framework.
- A new family of supply chain controls. The supply chain is one of the most vulnerable aspects of global commerce, and protecting it has been the goal of other recent NIST efforts.

Previous editions had a single supply chain control, but Revision 5 has an entire dedicated control family (Chapter 3.20).
- New, state-of-the-practice controls—such as those that support cyber resiliency and secure systems design—all based on the latest threat intelligence and cyberattack data.

The update is needed to help organizations maintain their defenses in the face of an ever-changing threat landscape.

"Revision 5 is important because threats, vulnerabilities and technology are evolving on a daily basis," said Dominic Cussatt, principal deputy assistant secretary and deputy chief information officer for the Department of Veterans Affairs. "It's critical for us that the controls remain up to date and agile."

NIST is planning a webcast in the future to help introduce users to the safeguards in the collection.

"We believe this is a world-class set of controls," Ross said. "It offers the greatest number of safeguards to protect the critical assets we use every day."

More information: undefined undefined. Security and Privacy Controls for Information Systems and Organizations, (2020). DOI: 10.6028/NIST.SP.800-53r5-draft

Provided by National Institute of Standards and Technology

safeguards.html