2021: What's Ahead from NIST in Cybersecurity and Privacy?

February 2, 2021
By: Kevin Stine

https://www.nist.gov/blogs/cybersecurity-insights/2021-whats-ahead-nist-cybersecurity-and-privacy

In 2020, NIST prioritized helping individuals and organizations shift to a more online environment to keep people safe and our economy productive. Despite the many challenges brought by the pandemic, we were fortunate to be able to continue our work on an array of new resources to help manage cybersecurity and privacy risks. As NIST looks ahead to the "new normal," we plan to build on lessons learned during the pandemic and to be even more strategic in anticipating and tackling the many challenges ahead.

We've made New Year's resolutions: to increase our attention on managing cybersecurity risks as part and parcel of the larger enterprise risk, to pay greater heed to the intersection between cybersecurity and privacy, to stress the cybersecurity of systems versus components, and to engage more forthrightly internationally and in our cross-cutting standards work.

So, what can government agencies, private sector organizations, and others who rely on NIST look forward to when it comes to assistance with cybersecurity and privacy-related matters in 2021? Here's a brief preview, organized to highlight our decision to focus on ***nine priority areas*** for the next several years.

We're fully engaged in our ***enhancing risk management*** initiative to produce a coordinated and cohesive portfolio of complementary resources that can be used individually or together to help public and private organizations at all levels of the enterprise. This spring we'll seek public comments on the Cybersecurity Framework (CSF) — how it's being used and how it could be improved. We won't be looking at the CSF in isolation. NIST will want to know how we might better mesh the CSF with the NIST Privacy Framework (PF), the NIST Risk Management Framework (RMF), and supply chain risk management approaches as well as with enterprise risk management (ERM). We also will issue CSF profiles for Positioning, Navigation, and Timing Services (final), election systems (draft), and the maritime sector (draft).

We'll soon propose a revision to "*Supply Chain Risk Management Practices for Federal Information Systems and Organizations*" (SP 800-161). That's a key NIST Cyber-Supply Chain Risk Management (C-SCRM) document relied upon heavily in the private and public sectors. And we're preparing to release a collection of key practices and recommended activities, and will share more information on a new forum for federal agencies and their contractors to convene and share ideas regularly on C-SCRM issues.

Among the other new and updated guidance federal agencies can expect are the final versions of *Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST SP 800-171* and a revision to NIST SP 800-53A, which provides procedures for assessing security and privacy controls. Comments are due in March to NIST's recently proposed revisions to the venerable *Security Guide for Interconnecting information Technology Systems* (SP 800-47), which adds much-needed emphasis on protecting information exchanged across organizations and the risk basis for information exchange decisions. Importantly, we are expanding the formats, sources, and data sets of our central security control catalogue to allow for tool users, developers, and automated techniques to take full advantage of this resource.

We're off to a quick start — literally — in the ***privacy*** arena in 2021, having released a quick start guide to the increasingly popular voluntary NIST *Privacy Framework*. Nominally for small and medium businesses, this guide can help any organization with constrained resources get a risk-based privacy program off the ground or improve an existing one. We've also released a much needed stakeholder-contributed crosswalk between the California Consumer Privacy Act (CCPA) and the Privacy Framework.

Strengthening cryptographic standards and validation has long been a mainstay of NIST's cybersecurity efforts, and 2021 will be no different. Examining new approaches to encryption and data protection that will protect from a quantum computer's assault, NIST's competition "selection round" will help the agency decide on the small subset of submitted algorithms that will form the core of the first post-quantum cryptography standard. NIST will move closer to releasing the initial standard for quantum-resistant cryptography, which will be unveiled in 2022. Before then, very likely this year, NIST will select winners in a competition to solicit, evaluate, and standardize lightweight cryptographic algorithms suitable for use in constrained environments where the performance of current NIST cryptographic standards is not acceptable.

With ***cybersecurity awareness, training, and education and workforce development*** more critical than ever, the NIST-led National Initiative for Cybersecurity Education (NICE) this year is stressing the importance of *Competencies* as a way to describe cybersecurity skills and to communicate between employers and learners. Stay tuned for the release of materials on those competencies to supplement the Workforce Framework for Cybersecurity (NICE Framework). NICE also will share an Implementation Plan for the NICE Framework goals — and begin to document progress.

Throughout the year, expect more details about our program on cybersecurity ***metrics and measurements***. We aim to support the development of technical measurements to determine the effect of cybersecurity risks and responses on an organization's objectives. Among other things, we will release an updated version of *Performance Measurement Guide for Information Security (SP 800-55 Revision 1)*. We also will continue to grow direct participation by industry in identifying and assigning metrics to the world's largest single repository of vulnerabilities in the National Vulnerability Database (NVD). And watch for an expansion of automated testing of encryption modules in our crypto testing and validation programs.

Identity and access management underlies so much of what's happening in cybersecurity right now. We're busy resolving public comments on FIPS 201 (the Standard behind the PIV Card and Derived PIV Credentials) and expect to produce a final revision this year. That "Revision 3" will expand the set of PIV credentials and allow remote supervised identity proofing — something that is especially important, as we learned during COVID-19 social distancing. It also will point to federation as the means for interoperability among agencies.

There's an urgent need to demonstrate the commercial viability of, and practical guidance for, secure IPv6-only enterprise deployment. With other agency and private sector collaborators at NIST's National Cybersecurity Center of Excellence (NCCoE), in 2021 we'll provide an approach and demonstrate the tools and methods for implementing IPv6, starting from an IPv6 in dual-stack mode and ending with an

IPv6-only network. It's one of many projects in our ***trustworthy networks*** focus area. So are NCCoE's 5G and Zero Trust cybersecurity efforts. In our 5G project, we are teaming with industry collaborators to integrate commercial and open-source products that leverage cybersecurity standards and recommended practices to showcase 5G's robust security features on trusted cloud infrastructure. And in our Zero Trust project, we'll be collaborating with industry to build out an example architecture that demonstrates a practical implementation of zero trust concepts and principles using commercially available products.

In the wide-ranging area of promoting ***trustworthy platforms***, our DevSecOps effort received an infusion of stakeholder support and guidance via two widely attended workshops in January. Findings from the sessions will help to integrate security into DevOps planning and processes and to inform new, practical and actionable guidance to fill any gaps, update existing guidance, and potentially develop NCCoE projects to demonstrate the practices.

There's no shortage of work to do to in ***securing emerging technologies***, and we're on it. IoT devices increasingly are integral elements of federal information systems, which is why NIST is eager for February 12th to arrive so we can see the public comments due on guidance drafts defining federal IoT cybersecurity requirements. These four documents released last December will expand the range of guidance for IoT cybersecurity, with the goal of ensuring IoT devices are integrated into the security and privacy controls of federal information systems. They will help address mandates in the recently enacted IoT Cybersecurity Improvement Act of 2020 and help ensure the government and IoT device manufacturers are on the same page.

That's only a fraction of the work we'll produce this year. As always, we strive for maximum input from the public and private sectors — you — so please respond to specific requests for your comments. But don't wait to be asked. Tell us what's on your mind and share your suggestions on Twitter via @NISTcyber.

ABOUT THE AUTHOR

Kevin Stine

Mr. Kevin Stine is the Chief of the Applied Cybersecurity Division in the National Institute of Standards and Technology's Information Technology Laboratory (ITL). He is also NIST's Acting Chief...