It Lurks Within: A Look at the Unexpected Security Implications of Compliance Programs

Rock Stevens and Michelle L. Mazurek | University of Maryland
Josiah Dykstra | Independent Researcher
Wendy Knox Everette | Leviathan Security Group

Compliance programs help protect organizations' intellectual property and valuable resources through mandated security controls; however, organizations often conflate compliance with strong security. Understanding the security gaps that place fully compliant organizations at risk is essential.

Digital security compliance programs standardize and enforce defensive controls against digital threats. Compliance programs are in place for handling credit card data, storing health information, or doing business with the government; failure to maintain compliance with mandated controls is typically followed by significant fines, loss of access to protected information, or employment termination. Although compliance standards may be carefully designed and thoroughly vetted during their creation, they are slowly and seldomly updated. Digital threats and countermeasures, on the other hand, change frequently. As a result, organizations that use compliance as a security checklist and consumers who use "compliant" products believing them to be secure, can quickly become vulnerable.

In response to the coronavirus pandemic, millions of people moved to online videoconferencing for work and school. Zoom, and other products like it, skyrocketed in popularity and usage. Hackers and security researchers quickly discovered security vulnerabilities in some of these services, including the ability to hijack meetings. CitizenLab also found that Zoom's cryptographic strength was less than advertised.[6] The U.S. Department of Defense, NASA, Google, and others banned the use of Zoom in response. Although Zoom is continually evolving its plans to bolster security,[3] this national-level attention on Zoom calls attention to a larger problem for the U.S. government.

Since April 2019, Zoom for Government has been compliant with the Federal Risk and Authorization Management Program (FedRAMP).[4] Achieving this authorization required adherence to a set of government-defined security controls for cloud-based services, but despite this certification, security issues remained, highlighting the danger in assuming that compliance implies security. FedRAMP is more comprehensive and flexible than many other compliance programs, yet dangerous gaps remain. For example, despite FedRAMP existing to protect government systems and information, no security control in FedRAMP prohibits cryptographic keys used by FedRAMP-compliant programs from being generated by a foreign nation. This could be exploited to allow a hostile nation to read sensitive information belonging to federal organizations and its employees.

As of 2020 May, FedRAMP has authorized 188 programs for use, with 49 additional programs currently in evaluation. FedRAMP's security (or lack thereof) impacts more than 5 million systems and devices across more than 150 government agencies. Given this scope, we felt compelled to dissect the controls within FedRAMP to understand their security gaps. Specifically, we wanted to identify the security controls that could lead to suboptimal security conditions within an organization despite being compliant with FedRAMP.

Digital Object Identifier 10.1109/MSEC.2020.3014291
Date of current version: 24 August 2020

After systematically analyzing FedRAMP's security controls, we identified 46 issues that may present security threats to organizations that use FedRAMP-approved programs. Additionally, we identified four threat models that appear to be neglected throughout FedRAMP and could pose significant threats if not properly handled.

Compliance Programs

Digital security compliance programs in the United States date back to the Computer Security Act of 1987, which required agencies to protect sensitive systems and conduct security training. Compliance programs should not be seen as a bulletproof solution for digital security; evidence shows that even fully compliant organizations can still suffer data breaches. For example, compliance auditors certified Target as payment card industry (PCI)-compliant in September 2013, just before it suffered a massive data breach in November 2013.

Extensive research has been conducted to better integrate compliance programs into an organization's policies, behavior, and even culture, but there continues to be limited focus on the inherent risks associated with actually being compliant.

We have previously studied security issues associated with digital compliance, identifying issues with the required controls as well as concerns that remain with even perfect compliance. Our team of cybersecurity experts audited three exemplar standards: Internal Revenue Service Publication 1075 (P1075), which protects taxpayer information; the PCI Data Security Standard (PCI DSS); which protects credit card data; and the North American Electric Reliability Corporation Critical Infrastructure Protection for system security management (CIP 007-6), which helps secure the country's electric grid. Not only did we identify 148 issues of varying severity across these standards, but we discovered no standardized process in place for responsible disclosure that might lead to their revision.[9]

Using the same audit methodology from this previous research, we systematically analyzed the "FedRAMP Security Controls Baseline" for security issues. We detail our findings for the "Moderate Baseline Controls" section, which was used to assess the security of Zoom for Government.

FedRAMP

FedRAMP is currently based on the NIST 800-53 Revision 4 Standard, which was originally published in April 2013 and updated in January 2015. A host of new threats to information security have emerged since this time: organizations have migrated toward bring-your-own-device strategies that let employees attach their personal devices to private networks and organizations have shifted from on-premises servers to the cloud, to name just two examples.

FedRAMP incorporates controls for a diverse set of security considerations, including several categories of protection. FedRAMP's control-naming convention uses the following two-letter category abbreviations combined with numbers to indicate the groupings of controls:

1. *access control* (*AC*): the security mechanisms that govern how systems and data are accessed
2. *audit and accountability* (*AU*): the requirements for assessing the implementation of controls
3. *identification and authentication* (*IA*): the mechanisms used for verifying users
4. *incident response* (*IR*): the programs and plans for handling security incidents
5. *media protection* (*MP*): the mechanisms used for protecting various storage devices
6. *physical and environmental protection* (*PE*): the requirements for safety and health
7. *risk assessment* (*RA*): the requirements for understanding risk and risk mitigation
8. *security assessment and authorization*: the controls used for conducting penetration tests
9. *system and communication protection* (*SC*): the controls utilized for ensuring privacy and availability
10. *system and information integrity* (*SI*): the controls used for data resiliency
11. *system and services acquisition* (*SA*): the controls and restrictions deployed for the procurement of digital systems and devices.

FedRAMP will likely adopt the NIST 800-53 Revision 5 Standard once it is finalized, but final draft comments were due in 2020 May. This slow pace of updating offers stability to cloud computing companies, which can design security and compliance programs to a known standard, but also potentially leaves new and emerging threats unmitigated.

So How Did FedRAMP Do?

Unfortunately, when we conducted a line-by-line audit of FedRAMP's controls we discovered a number of security concerns. Throughout FedRAMP, we focused on identifying the security controls or policies that can lead to suboptimal security conditions when implemented as written.

Each security concern we identified carries an associated risk. Frameworks such as the composite risk management framework (see Figure 1) calculate risk as a function of the probability of an event occurring and the severity associated with that event. Using this model, we can assess that a likely event with a negligible severity carries a low risk to an organization, while a likely event with a catastrophic severity (loss of life or significant financial loss) carries an extremely high risk to an organization.

Severity	Probability				
	Unlikely	Seldom	Occasional	Likely	Frequent
Catastrophic	M	H	H	E	E
Critical	L	M	H	H	E
Moderate	L	L	M	M	H
Negligible	L	L	L	L	M

Figure 1. Security risk levels. Levels were assigned based on a composite risk management risk-assessment matrix that includes both probability of occurrence and impact severity. E: extremely high; H: high; M: moderate; L: low.

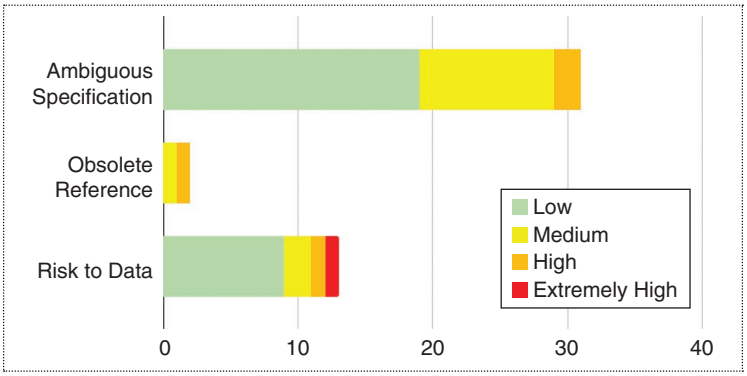

Figure 2. A distribution of the 46 security issues we identified within FedRAMP, by category.

In total, our audit of FedRAMP identified a total of 46 independent issues across 325 security controls. Of these, we determined that one issue presented an "extremely high" risk, four were rated as "high," 13 as "moderate," and 28 as "low" (see Figure 2). These 46 issues fall into three categories: an ambiguous specification, an obsolete reference, or a risk to data. In the following, we present detailed examples from these categories.

Ambiguous Specifications

Ambiguous specifications occur when two organizations can implement drastically different security controls and both are compliant; these types of issues represent the bulk of our findings. An example would be if ABC Company implements the control AC-06(09) for ensuring that an "information system audits the execution of privileged functions" by auditing after each individual occurrence, but the Widgets'R'Us company only conducts such audits every 60 days. Both companies are compliant—they both perform the mandatory audit—but ACME should be considered more secure. In the context of this example, an organization's interpretation and implementation of this control could be the difference between detecting a malicious threat during the initial stages of a compromise or only after attackers have already stolen sensitive victim data from the network.

FedRAMP uses certified third-party assessment organizations (3PAOs) as auditors to review and assess the FedRAMP compliance of any organization applying for authorization. The 3PAO, therefore, will be the primary arbiter of any ambiguous specifications or questionable implementations. Even though FedRAMP aims for all 3PAOs to operate with equal rigor, differences can arise. The 3PAO for ACME, for instance, may drill into the implementation details of the audit check as well as all functionality within ACME's system to ensure that all of its privileged functions are run through the same system audits. The 3PAO for Widgets'R'Us, meanwhile, may fail to dig deeply enough to catch that not all of Widgets'R'Us' functionality is audited, or it may fail to recognize that auditing privileged functions every 60 days is not compliant with the spirit of the control.

In total, we identified 31 unique issues involving ambiguous specifications: two high risk, 10 medium risk, and 19 low risk. We argue that inconsistencies in organizational and 3PAO interpretations of these controls may result in an increased threat to organizations using FedRAMP-compliant programs.

We identified 11 ambiguous specifications, with varying levels of risk, that fail to incorporate a time-based factor: how often should a task be performed or how soon after an event should a task be performed? A high-risk example includes AU-06(01), which requires an automated analysis of data artifacts to support investigations into suspicious activities. Examples of artifacts include records of every website a user visits, every time someone attempts to log in to a user account, or every time an antivirus program generates a suspicious activity alert. These artifacts, depending on the size of the network, could amount to billions of individual records and require 4–8 petabytes of storage a day. This control leaves up to the organization (and its 3PAO auditor) essential decisions like artifact-retention periods, correlation frequencies, and report availability. Given that advanced persistent threats can operate within networks for years before being detected, an organization must adopt a log-retention policy that would allow them to investigate compromises that may have occurred 6–12 months in the past.[11]

Correlation frequencies and report availability are intertwined; how often an organization aggregates and correlates data from network streams, end points, and service platforms directly shapes how soon they can process this data and provide a meaningful report that can support an investigation. Real-time processing can be a substantial monetary investment, but correlating petabytes of enterprise data from the past six months

from a cold start may take too long. Obviously there is a middle ground here, and we recommend the inclusion of a best-practice timeline for how often organizations should conduct data correlation for threat analysis.

There are 10 ambiguous specifications involving authentication mechanisms that may, under some interpretations, allow an attacker to gain access to resources. Two of these issues involve weak passwords. AC-18(01) protects wireless access to systems using authentication and encryption, but as-is would allow an organization to use encryption algorithms with known cryptographic weaknesses or trivially weak Wi-Fi authentication passwords, such as the letter "a." IA-05(04) requires password-strength checks using arbitrarily defined requirements (such as complexity and length) but does not compare user-generated passwords against common passwords or passwords found in data breaches. (For example, "P@$$Word123" passes most complexity checks but should not be used.) The Open Web Application Security Project and Have I Been Pwned? maintain repositories of commonly used passwords and account-breach data and provide interfaces for services to check passwords against; however, the use of services such as these is not required under any FedRAMP control. Understanding and mitigating the use of commonly used passwords and credential reuse across multiple accounts would improve the security of user accounts.

We found five issues involving multifactor authentication (MFA) and authenticators. These five controls permit SMS and email authenticator codes. Depending on the implementation, these additional layers of authentication may simply present additional hurdles that a capable attacker can likely bypass. SMS-jacking is a known attack vector that allows an adversary to port their victims' phone numbers to phones that the attacker controls, allowing them to receive victim SMS authenticator codes.[1] Attackers can also intercept unencrypted emails through man-in-the-middle attacks or traffic sniffing, allowing them to gain access to email-based authenticator codes. Hardware-based authenticators (such as YubiKeys or Titan Security Keys) and software authenticators (like those from Google Authenticator or Duo Security) have other complications but typically offer a much more secure approach to MFA.

Five controls permit organizations to provide their own definition of secure. AC-01 and AC-03 allow an organization to develop its own AC procedures and policies. These serve as the basis for most other controls within FedRAMP. Using an exaggerated example, imagine that ACME Company empowers an employee with 15 years of experience in AC to create its AC program while Widgets'R'Us subcontracts the task to the bagel vendor in the front lobby. As long as both companies produce the requisite documents, both are compliant, but ACME is more likely to have a robust program (who knows, maybe the bagel vendor is also a security expert who happens to love bagels).

Controls such as MP-07, IR-01, and AC-04 enable organizations to define what information is considered sensitive, how data can be exchanged between interconnected systems, and how the organization should conduct incident response investigations, respectively. None of these controls should be arbitrarily defined but rather rooted in best practices and iteratively updated after each internal evaluation, security exercise, or real-world data breach.

Obsolete References

Obsolete references occur when the document mandates the use of an outdated policy or references a document that has since been superseded; we found two instances of this in FedRAMP.

Throughout the document, FedRAMP references "FIPS Publications 140-2," which was replaced by 140-3 in September 2019. Additionally, IA-05(01) requires organizations to enforce password-expiration policies that NIST SP 800-63 has since rescinded; this high-risk issue is shown to encourage insecure practices such as writing newly rotated passwords near user workstations.[10] These two issues highlight a greater concern: FedRAMP has not been updated since August 2018. As technologies and best practices evolve over time, FedRAMP's authors must reconcile the need to remain secure with the requirement to remain adaptive. We recommend that compliance programs such as FedRAMP reference other security documents for best practices, but only the most recently updated versions.

Risks to Data

We have identified *risks to data*, defined as security controls that expose sensitive information to an attacker, as the category posing the greatest potential risk to organizations. In total, we found 13 risks to data: one extremely high, one high, two medium, and nine low-risk issues.

Organizations using FedRAMP-compliant solutions must consider who has access to protection mechanisms and how they can be accessed. AC-17(02) specifies the protection mechanisms used for remote access to systems. IA-05(02) details the requirements for public-key infrastructure-based authentication. SC-12 allows organizations to define requirements for key generation, distribution, storage, access, and destruction; SC-12(02) and SC-12(03) specify the requirements for symmetric and asymmetric keys, respectively. None of these controls mandate protection requirements for cryptographic keys. Given that FedRAMP relies on cryptographic keys for many security controls, an attacker can exploit this policy weakness to target and gain access to

unprotected cryptographic keys. We assess, in particular, that AC-17(02), which governs remote access to systems, would present an extremely high-risk situation for organizations if keys are not adequately protected.

MP-05(04) outlines the protection mechanisms used for media, but it does not include the protection mechanisms for keys or passwords used to encrypt the stored data. Sending passwords in cleartext emails or SMS would drastically reduce the efficacy of password-protected devices that have been intercepted by an adversary.

FedRAMP lacks oversight over the systems that provide security in an environment. Who is responsible for securing the security systems? SC-08(01) mandates that systems enforce data integrity checks during transmission but does not consider tamper controls against those checks. Consider two scenarios that could occur if an adversary gained control over an integrity checker: 1) they have the ability to enact a denial-of-service attack by flagging all in- and outbound traffic as corrupted, causing endless retransmissions of data; 2) they have the ability to modify content in transmission and verify its integrity, which could be exceptionally damaging to an organization if the attacker modified business records to annotate significant financial losses or fired an entire company via a cryptographically signed email.

SA-10(01) enforces integrity checks against software updates and patches but does not consider a compromised update server. In some situations, it may be appropriate to confirm the validity of updates from external vendors for critical networking devices, endpoint protection software, and workstations. These update servers are a juicy target for attacks, as they would give an adversary the ability to exploit an entire customer base from one system.

Similarly, RA-05(01) mandates the use of vulnerability scanners, and SI-03 dictates the use of malicious code scanners. Both solutions should be FedRAMP compliant and would require privileged access to data and systems to perform their intended functions. Neither solution is accounted for within FedRAMP as a potential threat vector. Attackers could manipulate these scanners to provide false negatives for alerts, allowing them to bypass defenses and gain access to vulnerable systems. These systems could also become an internal attack platform for adversaries taking advantage of their privileged, trusted access within the internal network. FedRAMP controls calling for antivirus software to be run on all systems similarly require running software that executes courtesy of privileged access on all systems, including some, such as Linux or Unix servers, where the antivirus software itself may create more of a risk than the actual chance of viruses attacking these platforms. Organizations should consider having tamper-resistant controls on all of the platforms that maintain elevated access within their networks and closely monitor them for deviation from normal behaviors.

Organizations must consider insider threats. For instance, AC-04 controls information flow between interconnected systems but provides for the local-network transmission of unencrypted controlled information. An insider threat or an adversary who has bypassed perimeter defenses could intercept these transmissions, placing controlled information at risk. As a best practice, sensitive information should always be encrypted at rest and in transit and protected by the appropriate restricted access controls. The use of role-based access controls or other restrictions that prevent viewing and manipulating data when not required for a user's current job should be in place. This kind of control can be implemented in a variety of ways and will be subject to interpretation by 3PAO auditors.

Expect the Unexpected: Ignored Threat Models

In analyzing the technical threats and trends across our results, we observe four threat models, or metalevel profiles of threat actors and their possible methodologies, that appear to be absent from FedRAMP's risk management considerations. These four threat models generically encompass the technical issues that we have identified and are helpful in framing the way that weaknesses in compliance standards can be taken advantage of by malicious actors. Abstracting the use of specific vulnerabilities into a threat model is a way that empowers defenders to identify and prioritize defenses against many adversaries and attacks. In the following, we discuss threats in terms of scope and motivation that we found undercut FedRAMP. Although we have focused on the risks to FedRAMP's certified cloud computing platforms and web-hosted software, improvement in other compliance programs can also be informed by these threat models.

Nation-State Privileged Access

Security issues and gaps, as exemplified throughout FedRAMP, present opportunities for foreign nations to access the private or sensitive data of compliant organizations. This may become more prevalent within the services provided by multinational corporations that provide encrypted solutions to a global customer base.

Private keys and passwords used for encrypting data must be protected from foreign-government access. Compliance loopholes that permit direct access to encryption keys and passwords could allow nation-states to bypass privacy controls. For example, a foreign government could mandate that companies generate encryption keys and store them in databases accessible to the company or the government on demand.

On-demand access would obviate encryption for data at rest or in transit, permitting foreign governments to decrypt information, at will, to conduct various forms of espionage that include intellectual property theft, personnel tracking, and communication eavesdropping.

Corporate Aggregation and Monetization

The second threat model considers businesses that desire to aggregate customer information for monetization. Knowing how customers use a service, from where they choose to use a service, when customers are most likely to use a service as well as knowing the issues encountered when using a service can all shape essential business decisions. Businesses can craft and deliver targeted ads, forecast inventory requirements, build security patches, or make future business-investment decisions based on this data. Most customers understand this is the status quo; however, we consider a threat model that exceeds the status quo and breaches customers' expectations of privacy by monetizing information that should be unreadable by the service provider.

In circumstances where companies identify loopholes in privacy laws or outright disregard privacy considerations, a company may be motivated to access the encrypted communications of their customers to further enrich known information. Issues such as the ones we discovered in FedRAMP could allow service providers to gain compliance and still bypass encryption. The ability to access private keys, remotely access account information, and clone MFA authenticators could enable an organization to impersonate users and farm information that can assist with further monetization.

Further, unless information is encrypted end to end and the software provider does not hold the encryption key—a relatively rare situation—user activity may be encrypted in transit and at rest yet still be processed by the service for targeted ads or personalized features. None of FedRAMP's encryption controls prohibit business access to private data and may present risks if sensitive information is disclosed. Although this concern is typically addressed during service contract negotiations, we feel it is important for compliance programs to explicitly address the issue.

Even though we highlight the issues related to corporations having too much user data, we must also consider the implications of denying certain information. Some companies use the user activity sent to them in to make software safer and more desirable for future purchases. One such example is Microsoft's use of customer stack traces, generated after crashes caused by users, to locate and fix security issues.[5] Organizations that are highly concerned about the confidentiality of their data may not allow these stack traces and other automated error reports to be automatically shared. (In our experience, many FedRAMP-compliant programs forego sharing stack traces for this very reason.) This excludes some of the most likely targets of sophisticated attacks from these automated vulnerability-detection programs, which may mean that exploits are detected only once they are used against other targets, potentially limiting their defensive effectiveness across the user base.

The examples discussed in this section demonstrate that compliance programs must reconcile the balance between service providers having too much user information and not enough. As is, both sides of the argument present risks to organizations that most reasonable users would not be willing to accept.

The Security of Security Appliances

In this third threat model, we consider attackers who are motivated to exploit security systems to bypass defenses and gain access to vulnerable systems. It is infeasible and inefficient for most companies to develop their own in-house security solutions or encryption mechanisms. For the most part, organizations rely on commercial security appliances or third-party service providers for their security. Inherently, the security of these applications have wide-reaching implications.

Security controls, such as those in FedRAMP, characteristically trust security applications and do not provide mechanisms for checks and balances. These applications require privileged access to data and systems without explicit oversight. Web proxies, for example, exist to reduce network bandwidth usage and provide security standoff from the Internet; but, these proxies may also have insight into all users' web traffic. Antivirus applications prevent the execution of malicious code on workstations; however, these applications may have the highest level of access to sensitive files and the core of the operating system.

The recent increase in remote work has made virtual private network (VPN) attacks even more attractive to malicious parties.[8] Although these attacks are not new,[7] the scale of users of these systems has greatly increased over the last few months, creating an enticing pool of targets. In the rush to move to remote work, many enterprises have neglected to ensure that their VPN servers are fully up to date, and these unpatched VPN servers provide a gateway to access corporate data that is otherwise unreachable. The VPN client software that runs on users' workstations and laptops provides another attack surface, particularly if the client software is out of date and has unpatched vulnerabilities. Both VPN servers and clients are security mechanisms often mandated by compliance programs that provide encrypted access to corporate information; however, the lack of explicit controls on protecting these protection mechanisms from compromise place organizations at risk.

We recommend a few methods to provide requisite security checks. First, monitoring and whitelisting the permitted behavior of these protection mechanisms may prevent hijacking; for example, the service-level account of the VPN server should not be allowed to access internal file shares after business hours. Site-reliability engineering provides many zero-trust recommendations that may help solve similar problems.[2]

Ignored Cyberphysical Systems

Digitally connected physical safety and security controls must also be included in an organization's security plan. As physical systems become more intertwined with information systems, we must actively mitigate the risks to organizations that could be posed by electric-power systems, closed-circuit television cameras, biometric scanners, or fire suppressors. Controls such as PE-13(03) from FedRAMP mandate that organizations use an automatic fire-suppression capability for information systems when a facility is not continually monitored. Consider the devastation that could occur if an attacker gained privileged access to a sprinkler system over a holiday and flooded the facility. An attacker could turn off power to essential services or expand its access within a network by using unprotected cyberphysical systems.

Not All Doom and Gloom

Compared with other compliance programs for protecting taxpayer information, credit card data, and the electric grid, we found fewer issues in FedRAMP. We largely attribute this to the vast number of listed collaborators, the frequent integration of lessons learned, and the use of public requests-for -comments, which allow interested parties to assess draft documents and provide recommended improvements. Additionally, FedRAMP mandates security controls based on three different levels of impact: low, moderate, and high. This acknowledges that systems and networks have different value and associated risk and should be protected accordingly. But as we discussed, such flexibility sometimes comes at the expense of underdefined or ambiguous specifications.

The maintainers of FedRAMP appear to have recognized some of the problems highlighted here, such as the varying interpretations of ambiguous specifications. FedRAMP partners with the American Association for Laboratory Accreditation to oversee its 3PAO program, and the two organizations have undertaken a process to review and update 3PAO training requirements and to evaluate the technical competence of 3PAOs. Additionally, these organizations have released standards that include a requirement that the 3PAOs that operate internationally show how they minimize the risk of foreign parties interfering with the FedRAMP certification process. A 3PAO that is operating under the influence of a foreign nation may, for instance, be more likely to be lenient in reviewing controls in certain areas that might make it easier for the foreign partner to attack systems or exfiltrate sensitive data.

Compliance programs like FedRAMP often contain security issues or gaps that can allow risks to persist, even in compliant organizations. We have provided tips and recommendations to help businesses, security researchers, and government organizations mitigate many of these risks. First and foremost, organizations and security professionals must remember that compliance establishes only a minimum level of protection. Compliance may be helpful (even required) to achieving the end goal of protecting an individual or organization's goals and assets, but it is not sufficient.

Organizations should understand the impact that compliance programs may have on overall security. We recommend that all organizations audit the compliance standards they follow to identify gaps that are relevant to their specific requirements and develop mitigating strategies accordingly.

As a whole, developing perfect compliance standards is an impossible task when you consider constantly evolving technologies and adversarial threats. The U.S. government must overcome its rigid processes and adopt a mechanism that permits always-open request-for-comment periods for compliance programs. This would allow security researchers to identify weaknesses and recommend fixes perpetually. For example, with open reporting, we would have the ability to properly disclose the four threat models previously discussed and design controls to address security gaps. Additionally, there is a need for faster revisions of compliance documents to maintain relevance with emerging technologies and threats. These revisions should permit grace periods, allowing organizations the time to migrate toward new controls without facing sanctions for noncompliance.

Additionally, there are opportunities to analyze 3PAO assessments to identify inconsistencies and provide clearer guidance to assessors. The U.S. government and its assessor accreditation partners can translate inconsistencies into training opportunities and also aid the development of automated scanning utilities to objectively assess security across all enterprises.

The coronavirus pandemic and the rapid adoption of work-from-home solutions such as Zoom only highlight the need for strengthening compliance programs. We hope our work can help make organizations, businesses, and citizens aware of potential security issues

until the federal government implements more secure and flexible options for compliance. ■

References

1. "Simjacker technical paper," AdaptiveMobile Security, Dublin. 2019. [Online]. Available: https://simjacker.com/downloads/technicalpapers/AdaptiveMobile_Security_Simjacker_Technical_Paper_v1.01.pdf
2. B. Beyer, C. Jones, J. Petoff, and N. R. Murphy, *Site Reliability Engineering: How Google Runs Production Systems*. Sebastopol, CA: O'Reilly Media, 2016.
3. J. Blum et al., "Zoom end-to-end encryption whitepaper," Github, San Francisco, White Paper, 2020. [Online]. Available: https://github.com/zoom/zoom-e2e-whitepaper
4. "Documents," FedRAMP, Washington, D.C., 2020. [Online]. Available: https://www.fedramp.gov/documents/
5. K. Herzig, "Improving software security with stack traces from bug reports," Microsoft, Redmond, WA, 2016. [Online]. Available: https://docs.microsoft.com/en-us/azure/devops/learn/devops-at-microsoft/improving-software-security-stack-traces-bug-reports
6. B. Marczak and J. Scott-Railton, "Move fast and roll your own crypto: A quick look at the confidentiality of zoom meetings," Citizen Lab, Toronto, 2020. [Online]. Available: https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/
7. "NSA cybersecurity advisory: Malicious cyber actors leveraging VPN vulnerabilities for attack; check VPN products for upgrade," National Security Agency, Ft. George G. Meade, MD, 2019. [Online]. Available: https://www.nsa.gov/News-Features/News-Stories/Article-View/Article/1982939/nsa-cybersecurity-advisory-malicious-cyber-actors-leveraging-vpn-vulnerabilities/
8. D. Palmer, "Hackers are scanning for vulnerable VPNs in order to launch attacks against remote workers," *ZDNet*, New York, 2020. [Online]. Available: https://www.zdnet.com/article/hackers-are-scanning-for-vulnerable-vpns-in-order-to-launch-attacks-against-remote-workers/
9. R. Stevens et al., "Compliance cautions: Investigating security issues associated with us digital-security standards," in *Proc. Network and Distributed System Security Symp.*, 2020. doi: 10.14722/ndss.2020.24003. [Online]. Available: https://www.ndss-symposium.org/wp-content/uploads/2020/02/24003-paper.pdf
10. L. Tam, M. Glassman, and M. Vandenwauver, "The psychology of password management: A tradeoff between security and convenience," *Behav. Inf. Technol.*, vol. 29, no. 3, pp. 233–244, 2010. doi: 10.1080/01449290903121386.
11. N. Virvilis, D. Gritzalis, and T. Apostolopoulos, "Trusted computing vs. advanced persistent threats: Can a defender win this game?" in *Proc. 2013 IEEE 10th Int. Conf. Ubiquitous Intelligence and Computing and 2013 IEEE 10th Int. Conf. Autonomic and Trusted Computing*, pp. 396–403. doi: 10.1109/UIC-ATC.2013.80.

Rock Stevens is a Ph.D. student in the Department of Computer Science at the University of Maryland researching human factors in digital security. Stevens received his M.S. in computer science from the University of Maryland. His research interests include understanding best practices within digital security and making them better. Contact him at rstevens@cs.umd.edu.

Michelle L. Mazurek is an associate professor in the Department of Computer Science and the Institute for Advanced Computer Studies at the University of Maryland. Her research interests include understanding and building tools and interventions for improving security- and privacy-relevant decision making. Mazurek received her Ph.D. in electrical and computer engineering from Carnegie Mellon University. Contact her at mmazurek@umd.edu.

Josiah Dykstra is an independent security researcher. Dykstra received his Ph.D. in computer science from the University of Maryland, Baltimore County. His research interests include cybersecurity science, human factors and resilience in cyber, and economics of cybersecurity. Contact him at josiahdykstra@acm.org.

Wendy Knox Everette is a senior security advisor at Leviathan Security Group, Seattle, Washington. Everette received her B.A. in media arts and sciences from Wellesley College. Her research interests include information security, cloud computing, and usable security. Contact her at wknox@wellesley.edu.