Guidehouse
Outwit *Complexity*

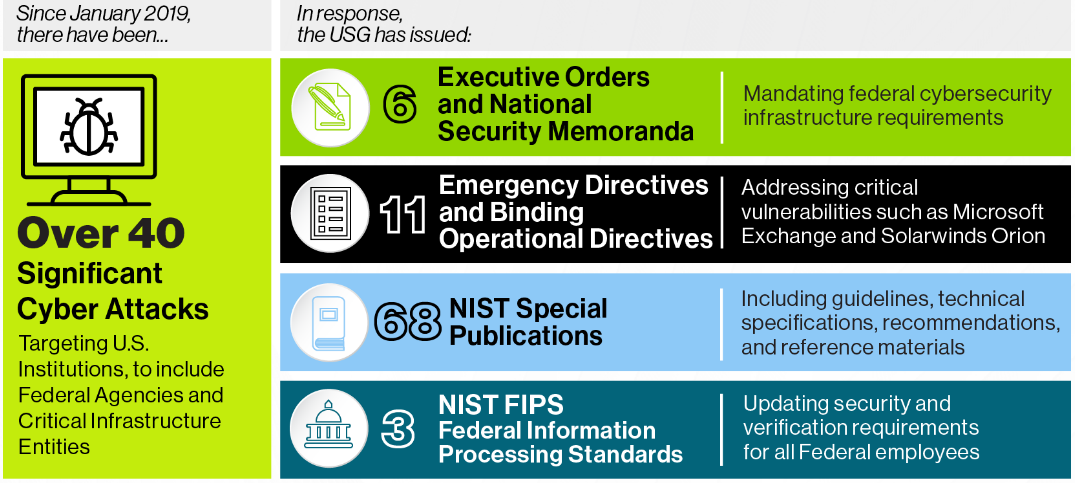
guidehouse.com

Combating the Evolving Threat Landscape with a Dynamic Cybersecurity Policy Program

The President's Executive Order (EO) 14028 on "Improving the Nation's Cybersecurity" is the culmination of years of demand for the United States Government to take a more active approach in addressing our Nation's cybersecurity challenges. The EO introduces measures aimed at improving threat intelligence sharing, supply chain security, and modernizing the cybersecurity architecture across Federal agencies.

With this EO, the Government has issued ten instances of authoritative guidance and dozens of standards over the past two and a half years. Federal entities have the challenge of implementing cybersecurity policies and supporting unique missions while keeping pace with an evolving cybersecurity threat landscape. Developing a mature cybersecurity policy program that can address this challenge is dependent on engaging key organizational stakeholders, consistently refining policy and organizational guidance, and developing a forward-leaning cybersecurity culture.

As cyberattacks have increased both in sophistication and volume, the number and complexity of Federal measures released in response has risen as well (Figure 1), including the far-reaching EO 14028. Agencies must balance compliance with, redundant guidance from multiple Government organizations at times, while retaining the freedom to adapt as needed to accomplish their specific missions. A robust and mature cybersecurity policy program is crucial to the ability of agencies to effectively strike this balance and efficiently address cybersecurity threats to their organizations and missions.



Since January 2019, there have been...

Over 40 Significant Cyber Attacks Targeting U.S. Institutions, to include Federal Agencies and Critical Infrastructure Entities

In response, the USG has issued:

6 Executive Orders and National Security Memoranda | Mandating federal cybersecurity infrastructure requirements

11 Emergency Directives and Binding Operational Directives | Addressing critical vulnerabilities such as Microsoft Exchange and Solarwinds Orion

68 NIST Special Publications | Including guidelines, technical specifications, recommendations, and reference materials

3 NIST FIPS Federal Information Processing Standards | Updating security and verification requirements for all Federal employees

Figure 1 outlines the number of significant cyberattacks against U.S. institutions since 2019 and the ensuing Federal measures issued to improve the security postures of Government agencies.

Involving Key Stakeholders

In June 2021, the Senate confirmed the nation's first National Cyber Director. The appointment is intended to consolidate Federal cybersecurity coordination efforts, and the National Cyber Director will be expected to oversee cybersecurity programs across the Federal government. Much like the National Cyber Director, agency Chief Information Officers (CIO) and Chief Information Security Officers (CISO) are expected to be the driving force behind their organization's cybersecurity policy development and implementation. However, it is critical that they coordinate the involvement of key stakeholders from across the organization throughout the process.

Engagement from leadership across teams such as finance, legal, privacy, human resources, and agency executives promotes commitment to the policy's successful development and implementation. During the development process, individuals representing their office should be prepared to discuss the learnings, shortcomings, and sustainable measures of prior policies; These candid conversations can help drive to create/establish an end policy that can realistically balance a risk-based approach while also meeting various Federal cybersecurity requirements.

With the business stakeholders' and the CIO/CISO office collaborative efforts, the process enables an agency to establish common understanding and compliances standard. It helps standardize policy language and set policy priorities that meet both internal policy directives and Federal measure. Some specific considerations that a mature cybersecurity policy program should address include:

Resource allocations

- How can the agency best allocate existing resources (budget, human capital, etc) in responding to new Federal cybersecurity guidelines?
- Are new resource allocations required to comply with this new Federal cybersecurity guidelines or cybersecurity policy, or can the agency address it through augmenting/enhancing current assessments or activities?
- What additional human capital resources and skillsets may be needed to accomplish the cybersecurity mission and implement applicable Federal cybersecurity directives?
- From a procurement standpoint, what are the systems, software, hardware, etc. that must be acquired by the agency to be well positioned to respond to new Federal cybersecurity directives and future cybersecurity incidents?

Training & Reporting

- What are the legal considerations that must be considered when implementing future Federal measures, such as reporting guidelines or EOs? Are there any specific privacy considerations to consider?
- How can the agency continuously educate employees on internal cybersecurity policy? How will checks on learning and compliance be conducted across different levels of the organization?

Policy Implementation and Continuous Refinement

The best and most effective policies are actively practiced, refined and enhanced. Agency leadership should conduct regular checks across their organizations to promote continued compliance with internal policies and Federal guidelines. As part of the policy development process, organizations should identify what type of monitoring is needed to ensure this compliance, establish a clear governance structure for overseeing this process, and define performance measures to consistently evaluate policy impact. Compliance may assess functions such as the implementation of security controls around critical assets in accordance with cybersecurity risk quantification processes, as well as reviewing security-specific metrics such as incident response times across the organization.

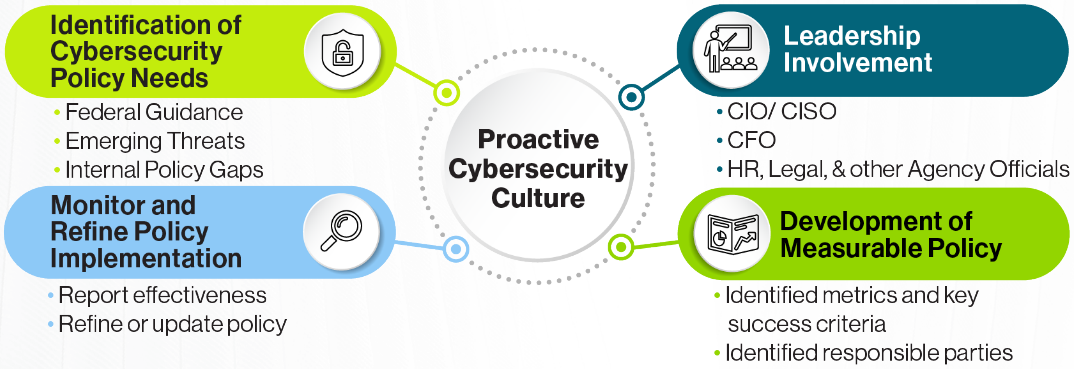
Leaders needs to be mindful of their agencies deficiency in key policy areas and identify opportunities for improvement in the cybersecurity policies compliance implementation. Additionally, organizational leaders must ensure that the stakeholders continue to stay abreast of new technology and evaluate the applicability that may necessitate new policies or updates to existing policies.

As the threat landscape is constantly evolving, effective cybersecurity governance needs to be under continuous evaluation. Organizations may consider scheduling recurring quarterly or monthly meetings with key personnel to review and refine their cybersecurity policy, determine if any of the changes to their cybersecurity program may impact other standing policies. Ultimately, a mature program that is continuously refined will have the ability to adjust to new Federal cybersecurity guidelines with agility and minimize any disruption at the release of time-sensitive Federal mandates.

Developing a Proactive Cybersecurity Culture

Organizations must work to develop a proactive cybersecurity culture to appropriately address agency and industry-specific cybersecurity concerns and applicable cybersecurity regulations. Change across any organization always begins at the top. Involving leaders from across the agency in the cybersecurity policy planning process can instill a forward-thinking attitude towards cybersecurity that trickles down across their teams. Successful implementation of a sustainable cybersecurity policy ultimately involves fostering a proactive culture around cybersecurity across the organization.

A forward-leaning cybersecurity program can help agencies prepare and adapt swiftly to emerging risks and threats. Thoughtful and sensible guidance at this level helps to guide internal decision-making through insights gleaned from strong internal programs. Furthermore, a proactive policy program creates a desired workforce culture that can help prevent major breachers across department and agencies by practicing strong cybersecurity hygiene.



Identification of Cybersecurity Policy Needs
• Federal Guidance
• Emerging Threats
• Internal Policy Gaps
Monitor and Refine Policy Implementation
• Report effectiveness
• Refine or update policy
Proactive Cybersecurity Culture
Leadership Involvement
• CIO/ CISO
• CFO
• HR, Legal, & other Agency Officials
Development of Measurable Policy
• Identified metrics and key success criteria
• Identified responsible parties

Figure 2 illustrates the framework for the utilization of a robust, mature, forward leaning, and adaptive cybersecurity policy program to promote and maintain a proactive cybersecurity culture.

Guidehouse
Outwit *Complexity*

Proactive Cybersecurity Culture

Organizations must work to develop a proactive cybersecurity culture to appropriately address agency and industry-specific cybersecurity concerns and applicable cybersecurity regulations. This culture requires engagement and enablement of leaders tasked with cybersecurity decision-making responsibilities and additional organizational leadership as well as those executing cybersecurity policy. A proactive cybersecurity culture also requires actionable and measurable cybersecurity policy as well as continuous monitoring, review, and refinement of those policies informed by benchmarking of best practices from other agencies or industries and diligent awareness of emerging threats and regulatory requirements.

Email: nationalsecurity@guidehouse.com / **Web:** guidehouse.com / @guidehouse linkedin.com/company/guidehouse