DoD Digital Modernization Strategy (2019)

The Foreword sets the tone for the DoD Digital Modernization Strategy, emphasizing the urgency of modernizing infrastructure to maintain technological dominance and address growing cyber threats. However, when cross-referenced with EO 13800 and the NIST Cybersecurity Framework (NIST CSF), several areas show partial alignment, while others reveal critical gaps.

EO 13800 explicitly mandates that federal agencies adopt the NIST CSF to improve the resilience of critical infrastructure and ensure comprehensive risk management. The foreword's focus on modernization and cybersecurity suggests alignment with these principles. Still, the absence of explicit reference to EO 13800 or the NIST CSF raises concerns about the strategy's commitment to these frameworks. For instance, the foreword lacks a direct acknowledgment of the five core functions of the NIST CSF—identify, protect, detect, respond, recover—which are foundational to meeting EO 13800's risk management objectives. Instead, the language remains high-level, prioritizing modernization without providing the operational context needed for compliance.

Similarly, the Executive Summary outlines ambitious goals such as enhancing enterprise visibility, adopting zero-trust principles, and leveraging advanced technologies like artificial intelligence and cloud computing. These initiatives align broadly with modernization objectives, yet they fall short of addressing the granular requirements of NIST SP 800-53, 800-30, and 800-37, which emphasize specific risk management practices. For example, while the summary mentions "enterprise integration," it does not clarify whether this includes robust risk assessments or continuous monitoring practices, both of which are critical under NIST SP 800-37's Risk Management Framework (RMF).

Furthermore, EO 13800 underscores the importance of securing critical infrastructure sectors, requiring clear accountability and measurable progress. The Executive Summary's emphasis on innovation and optimization lacks concrete metrics or timelines for achieving cybersecurity milestones. For instance, while zero-trust principles align with NIST SP 800-207, the strategy does not detail how these principles will be implemented or measured. This lack of specificity raises questions about how the DoD plans to operationalize these goals in compliance with EO 13800 and the NIST CSF.

The strategy's mention of artificial intelligence and cloud adoption indirectly ties to NIST SP 800-161, which focuses on supply chain risk management. However, the summary does not address how these technologies will be evaluated for risks posed by untrusted vendors or insecure supply chains. This omission suggests a gap in

aligning with the comprehensive risk management practices outlined in NIST SP 800-161.

The Foreword and Executive Summary establish a vision of modernization and cybersecurity but lack the operational clarity and specific references necessary for full compliance with EO 13800 and NIST standards. While the strategy aligns conceptually with principles like zero trust and enterprise integration, it falls short of detailing how these objectives will be implemented in a manner consistent with NIST SP 800-53, 800-171, 800-30, and 800-37. This lack of specificity leaves significant gaps in demonstrating compliance with federal mandates.

The Goals and Objectives section of the DoD Digital Modernization Strategy outlines ambitious plans to address modernization and cybersecurity challenges. These goals broadly align with the priorities set forth in EO 13800 and the principles of the NIST Cybersecurity Framework (NIST CSF). However, the strategy lacks the granularity required to demonstrate compliance with the specific mandates of EO 13800 and the related NIST SP 800 series standards.

The goal of enhancing cybersecurity is central to the strategy and aligns conceptually with EO 13800's mandate to secure critical infrastructure through risk-based practices. However, the strategy does not explicitly reference key components of NIST SP 800-53 or the NIST CSF. For example, the emphasis on "zero-trust principles" is a strong starting point, aligning with the principles outlined in NIST SP 800-207. However, the strategy does not provide clear implementation paths for achieving the full spectrum of NIST CSF core functions—identify, protect, detect, respond, and recover. This omission leaves gaps in how the DoD will operationalize zero-trust and address broader cybersecurity risks.

In terms of IT optimization, the strategy focuses on modernizing legacy systems, which aligns with EO 13800’s directive to improve federal IT infrastructure. However, the absence of detailed controls or measures tied to NIST SP 800-171 for protecting Controlled Unclassified Information (CUI) within these systems is a critical oversight. Additionally, while the strategy highlights the benefits of cloud adoption, it does not detail how these systems will meet compliance with SP 800-161, particularly regarding supply chain risk management. EO 13800 explicitly requires agencies to ensure the resilience of critical infrastructure, including the IT backbone, but the strategy does not discuss continuous monitoring, vulnerability management, or risk-based metrics for success.

The goal of leveraging data and artificial intelligence (AI) reflects a forward-thinking approach, emphasizing the importance of innovation for operational effectiveness. However, this goal neglects critical aspects of NIST SP 800-161, which emphasizes securing data integrity throughout the supply chain. AI systems are particularly

vulnerable to adversarial attacks, and the strategy does not address measures to prevent or mitigate risks such as data poisoning or model manipulation. EO 13800 requires agencies to manage risks associated with critical systems, yet the strategy does not provide a framework for evaluating AI-specific risks or ensuring compliance with relevant standards.

The focus on workforce development aims to address the growing demand for skilled cybersecurity personnel. This aligns conceptually with EO 13800's emphasis on building a robust cybersecurity workforce. However, the strategy does not specify how training programs will integrate NIST CSF principles or address the requirements of SP 800-53 related to personnel security. For instance, EO 13800 calls for measurable progress in developing cybersecurity talent, but the strategy lacks concrete metrics or benchmarks for evaluating the effectiveness of workforce initiatives.

In addition to these gaps, the strategy does not address incident response readiness, a critical component of NIST SP 800-53 and the NIST CSF. EO 13800 requires agencies to prepare for and respond to cyber incidents effectively. While the strategy mentions enhancing cyber resilience, it does not outline plans for incident response testing, tabletop exercises, or post-incident evaluations, leaving a significant gap in compliance.

The Goals and Objectives section provides a high-level vision for modernization but lacks the detailed implementation plans and compliance measures needed to meet the mandates of EO 13800 and the NIST standards. The focus on cybersecurity, IT optimization, data and AI, and workforce development is commendable, but the absence of specific references to NIST SP 800-53, 800-30, 800-37, 800-161, and 800-171 undermines its ability to ensure measurable and accountable progress. Without concrete actions tied to these standards, the strategy risks falling short of its stated objectives and federal requirements.

The Strategic Elements section establishes the foundational principles guiding the Department of Defense's digital modernization. These principles—innovation, security, scalability, and interoperability—are essential for achieving modernization goals. However, upon closer examination and cross-referencing with EO 13800 and the NIST SP 800 series standards, significant gaps emerge, particularly in operationalizing these principles in compliance with federal mandates.

The principle of innovation is forward-looking and emphasizes the need to outpace adversaries by adopting emerging technologies. This aligns conceptually with EO 13800's call for modernizing federal IT systems to ensure resilience and competitiveness. However, innovation inherently carries risks, particularly in the rapid adoption of unvetted technologies or third-party components. NIST SP 800-161

addresses supply chain risk management, requiring organizations to evaluate and mitigate risks from untrusted vendors or insecure components in technology acquisition. The strategy fails to outline a structured framework for assessing these risks, leaving a compliance gap. Moreover, innovation without robust security controls can inadvertently introduce vulnerabilities, contradicting the intent of NIST SP 800-53 and SP 800-30, which emphasize balancing innovation with risk assessment and control implementation.

The principle of security is presented as a cornerstone of the strategy. It prioritizes protecting the Department's assets and infrastructure against a constantly evolving threat landscape. While this aligns broadly with the NIST CSF and EO 13800's directives, the lack of explicit reference to the five core functions of the NIST CSF—identify, protect, detect, respond, recover—indicates a superficial approach. For example, the strategy emphasizes the adoption of zero-trust principles, which are consistent with NIST SP 800-207, but it does not address how zero trust will be implemented across legacy systems or integrated into new technologies. Similarly, EO 13800 mandates risk-based approaches to critical infrastructure protection, yet the strategy does not provide specific measures for conducting comprehensive risk assessments or implementing security controls, as required by SP 800-53 and SP 800-37.

The principle of scalability reflects the Department's focus on ensuring that its digital infrastructure can adapt to changing operational demands. This is critical for maintaining readiness in dynamic and resource-intensive environments. However, scalability often introduces challenges related to security and compliance. For example, as systems scale, the potential for vulnerabilities increases, particularly in cloud environments. NIST SP 800-171 emphasizes protecting Controlled Unclassified Information (CUI) in nonfederal systems, yet the strategy does not detail how scalable solutions will meet these requirements. Similarly, EO 13800's emphasis on securing IT systems during modernization is undermined by the absence of plans for continuous monitoring and vulnerability management in scalable systems, as outlined in SP 800-53 and SP 800-161.

The principle of interoperability is critical for ensuring seamless communication and data sharing across the Department's systems and with external partners. While this aligns with EO 13800's goal of improving the efficiency and effectiveness of federal IT systems, increased interoperability also introduces significant security challenges. NIST SP 800-53 and SP 800-37 emphasize the importance of continuous monitoring, risk assessments, and robust access controls in interconnected systems. The strategy does not provide detailed measures for addressing these challenges, nor does it outline how interoperability will be balanced with the need for strong access controls and data protection. The absence of specific plans for securing interoperable systems represents a critical gap in compliance.

One significant omission in the Strategic Elements section is the lack of focus on measurable outcomes and accountability. EO 13800 requires agencies to track and report progress in implementing cybersecurity measures, including aligning with the NIST CSF and other federal standards. The strategy's principles are high-level and aspirational, but without concrete metrics or benchmarks, it is impossible to assess progress or ensure compliance. For example, the principle of security could be operationalized through measurable goals such as reducing the time to detect and respond to threats or increasing the percentage of systems compliant with SP 800-171. Similarly, scalability could be tracked by measuring the percentage of legacy systems successfully migrated to secure cloud environments.

The Strategic Elements section provides a conceptual foundation for digital modernization but lacks the specificity and operational clarity required to comply with EO 13800 and the NIST SP 800 series standards. While the principles of innovation, security, scalability, and interoperability are essential, the absence of detailed implementation plans, risk assessments, and measurable outcomes leaves significant gaps in demonstrating compliance. To achieve the goals set forth in EO 13800, the strategy must explicitly address the requirements of NIST SP 800-53, SP 800-30, SP 800-37, SP 800-161, and SP 800-171, ensuring that each principle is operationalized with clear metrics and accountability mechanisms.

The Key Initiatives and Cybersecurity Framework section of the DoD Digital Modernization Strategy reflects an ambitious vision for modernizing the Department's infrastructure and capabilities. The initiatives—spanning cloud technology, artificial intelligence, data management, and advanced cybersecurity—are central to achieving the strategy's goals. However, when examined against the specific requirements of EO 13800 and the NIST standards, critical gaps become evident, particularly in the operationalization and compliance mechanisms necessary to meet federal mandates.

The emphasis on cloud technology as a cornerstone of modernization is well-aligned with EO 13800's focus on improving federal IT infrastructure. Yet, the strategy fails to address the inherent risks associated with cloud adoption. It does not explicitly detail how cloud environments will adhere to NIST SP 800-171 requirements for protecting Controlled Unclassified Information, nor does it outline measures to ensure compliance with NIST SP 800-53 security controls. The mention of "enterprise cloud solutions" suggests a broad adoption strategy, but the absence of specifics—such as encryption protocols, secure configuration standards, and continuous monitoring—creates uncertainty about how these deployments will meet the security expectations outlined in EO 13800.

The risks posed by third-party vendors and supply chains in cloud environments are similarly underdeveloped. Supply chain vulnerabilities, a significant concern in modern IT systems, are comprehensively addressed in NIST SP 800-161. Yet, the strategy does not provide a framework for evaluating vendor risks or managing untrusted components. This omission is particularly concerning given the reliance on external providers for cloud services. Without a structured approach to mitigating supply chain risks, the strategy leaves critical gaps in compliance with EO 13800's requirements to secure federal IT against external threats.

Artificial intelligence, positioned as a transformative tool for defense operations, presents its own set of challenges. The strategy highlights AI as a key initiative but does not address the unique vulnerabilities associated with these systems. Risks such as adversarial attacks, data poisoning, and biases in training models are well-documented concerns in AI security. While NIST SP 800-53 and SP 800-161 provide guidance on mitigating such risks, the strategy does not explain how these standards will be applied in AI development and deployment. Furthermore, the lack of specific measures to secure AI inputs and outputs, test model robustness, or monitor system performance undermines the Department's ability to meet EO 13800's emphasis on risk-based cybersecurity approaches.

Data management and interoperability are critical enablers of the Department's operational efficiency. However, increased data sharing and system integration come with heightened risks. While the strategy emphasizes the importance of interoperability, it does not address how these interconnected systems will be secured. NIST SP 800-53 and SP 800-37 stress the need for continuous monitoring, robust access controls, and secure data transmission in interoperable environments. The strategy's lack of specifics on these measures leaves significant vulnerabilities unaddressed. EO 13800's mandate to secure critical infrastructure is at odds with this omission, as seamless data sharing without proper safeguards could expose sensitive information to adversaries.

Cybersecurity enhancements are at the heart of the strategy, with a focus on zero-trust principles and cyber resilience. These initiatives align with modern cybersecurity practices and the intent of NIST SP 800-207, which provides a framework for implementing zero-trust architectures. However, the strategy does not delve into the practicalities of applying zero trust across legacy systems and emerging technologies. Zero trust requires strict access controls, micro-segmentation, and real-time monitoring—all of which are integral to NIST SP 800-53—but the strategy lacks detail on these implementation aspects. Similarly, the absence of a clear framework for incident response and recovery planning represents a critical gap. Both EO 13800 and the NIST CSF emphasize the importance of robust response capabilities, yet the strategy does not outline plans for testing, refining, or evaluating its incident response measures.

The Cybersecurity Framework subsection further highlights these shortcomings. While the strategy references risk-based approaches, it does not explicitly map its initiatives to the five core functions of the NIST CSF: identify, protect, detect, respond, and recover. For instance, asset inventory and risk assessments, central to the “identify” function, are not clearly outlined. Similarly, the “respond” and “recover” functions, which rely on incident response and business continuity planning, are not adequately addressed. This lack of alignment with the NIST CSF underscores a broader issue: the strategy’s high-level goals are not supported by detailed, actionable plans that ensure compliance with EO 13800 or the NIST standards.

In essence, while the Key Initiatives and Cybersecurity Framework section articulates a forward-looking vision for modernization, it falls short of providing the operational clarity and specificity required to meet federal cybersecurity mandates. The absence of detailed implementation plans, risk assessments, and measurable outcomes leaves significant gaps in compliance. To address these issues, the strategy must explicitly incorporate the requirements of NIST SP 800-53, SP 800-171, SP 800-37, SP 800-161, and the NIST CSF, ensuring that each initiative is operationalized with clear metrics, accountability mechanisms, and a focus on continuous improvement. Without these enhancements, the strategy risks leaving critical vulnerabilities unaddressed, undermining its overall effectiveness and compliance with EO 13800.

The IT Modernization and JIE section outlines the DoD's strategy for consolidating and improving its IT infrastructure, emphasizing efficiency, scalability, and cybersecurity. These objectives are foundational for a modern defense environment, but their alignment with EO 13800 and the NIST SP 800 series standards reveals critical areas requiring additional clarity, operational detail, and compliance.

The strategy’s emphasis on replacing outdated systems is a necessary step for addressing vulnerabilities associated with legacy infrastructure. Outdated systems often lack support for modern security protocols, making them high-risk entry points for adversaries. While EO 13800 highlights the importance of modernizing IT infrastructure, the DoD strategy does not sufficiently address interim controls for securing legacy systems until their decommissioning. For example, NIST SP 800-30 emphasizes the importance of assessing and mitigating risks associated with aging systems. Without interim safeguards—such as segmentation, access restrictions, or enhanced monitoring—these systems could undermine the broader modernization efforts. The omission of such details leaves an operational gap that should be addressed to ensure compliance with both EO 13800 and NIST standards.

The integration of cloud services is a centerpiece of the IT modernization plan, aimed at improving scalability and enabling rapid deployment of resources. This aligns with

EO 13800's call to modernize federal IT systems, yet the strategy does not provide sufficient detail on the security measures necessary for compliance with NIST SP 800-171 and SP 800-53. For example, cloud environments handling Controlled Unclassified Information (CUI) must implement specific controls such as encryption for data at rest and in transit, multifactor authentication, and continuous monitoring. The strategy's high-level mention of cloud adoption does not address these critical controls or explain how vendor compliance with these standards will be ensured. The risks associated with cloud vendors, including potential backdoors or supply chain vulnerabilities, are significant, as highlighted in NIST SP 800-161. By failing to include a framework for vetting cloud providers or managing risks associated with third-party services, the strategy leaves a compliance gap in one of its most critical modernization areas.

The Joint Information Environment (JIE) is positioned as a transformative initiative for improving data sharing and operational collaboration across the DoD. While the goal of enhanced interoperability aligns with EO 13800's objectives of improving efficiency, it introduces heightened risks related to system interconnectivity. Interoperability increases the attack surface, as vulnerabilities in one system can cascade across interconnected networks. NIST SP 800-53 and SP 800-37 emphasize the need for robust controls in interconnected environments, including secure access controls, network segmentation, and real-time monitoring. The DoD strategy mentions these principles broadly but does not provide specific implementation details. For example, how will access controls be enforced across the JIE? Will there be a centralized identity management system to prevent unauthorized access? The lack of specificity in addressing these concerns undermines the strategy's alignment with EO 13800 and the NIST Cybersecurity Framework (NIST CSF).

One of the most significant omissions in the IT Modernization section is a comprehensive plan for continuous monitoring and vulnerability management. EO 13800 mandates that federal agencies adopt risk-based approaches to securing their IT infrastructure, which requires real-time visibility into system vulnerabilities and threats. NIST SP 800-37 outlines a Risk Management Framework (RMF) that integrates continuous monitoring as a critical component of maintaining system security. While the strategy mentions monitoring as part of its cybersecurity efforts, it does not detail how this will be implemented across the DoD's IT environment. Questions such as which tools will be used, how monitoring data will be analyzed, and how responses will be coordinated remain unanswered, leaving a critical gap in operationalizing this essential function.

The strategy also fails to adequately address incident response capabilities during the modernization process. Transitioning to modern systems inevitably introduces periods of increased risk, as configurations are updated and new vulnerabilities may be exposed. EO 13800 and NIST SP 800-53 both emphasize the importance of having

robust incident response plans in place to mitigate these risks. The absence of explicit plans for testing, refining, and deploying incident response measures during the modernization process represents a significant oversight. For example, there is no mention of tabletop exercises, red-teaming, or other proactive measures that could ensure readiness in the event of a breach.

Another critical area is the lack of a clear roadmap for achieving measurable outcomes. EO 13800 requires agencies to demonstrate progress in meeting cybersecurity objectives, yet the strategy does not provide metrics or benchmarks for assessing the success of IT modernization efforts. For instance, how will the DoD measure improvements in system availability, data security, or operational efficiency? Without concrete metrics, it is difficult to evaluate whether the modernization initiatives are achieving their intended goals or meeting compliance standards. NIST SP 800-53 emphasizes the need for measurable controls, and integrating these into the strategy would significantly enhance its alignment with federal mandates.

Lastly, the strategy does not sufficiently address the human element of IT modernization. Transitioning to modern systems requires not only technical updates but also workforce training to ensure that personnel can effectively manage and secure the new infrastructure. NIST SP 800-53 includes requirements for personnel security, emphasizing the importance of training and awareness programs. While the strategy touches on workforce development in other sections, it does not link this directly to IT modernization, leaving a gap in ensuring that the workforce is adequately prepared for the challenges of a modernized IT environment.

The IT Modernization and Joint Information Environment (JIE) section outlines an ambitious vision for transforming the DoD's IT landscape, but it lacks the operational depth and compliance mechanisms necessary to meet the mandates of EO 13800 and the NIST SP 800 series standards. While the strategy aligns conceptually with modernization objectives, it falls short in addressing critical areas such as interim security for legacy systems, cloud compliance, continuous monitoring, incident response, and workforce readiness. The absence of detailed implementation plans and measurable outcomes leaves significant gaps in compliance with NIST SP 800-53, SP 800-171, SP 800-37, and SP 800-161. To fully align with federal requirements, the strategy must provide a more detailed roadmap that includes specific security controls, risk management processes, and accountability mechanisms. Without these enhancements, the modernization efforts risk being undermined by unaddressed vulnerabilities and operational inefficiencies.

The Appendices and Supporting Material section of the DoD Digital Modernization Strategy serves as a repository for additional context, frameworks, and methodologies that underpin the main strategy. This section is expected to provide the granular details and technical references necessary to operationalize the broader goals of

modernization and cybersecurity. However, when analyzed in the context of EO 13800 and the NIST SP 800 series standards, several critical gaps and omissions emerge, underscoring potential deficiencies in the strategy's implementation.

One of the most striking omissions in the appendices is the lack of explicit mappings to compliance frameworks such as the NIST Cybersecurity Framework (NIST CSF) and key publications like NIST SP 800-53, SP 800-37, SP 800-161, and SP 800-171. EO 13800 mandates the adoption of the NIST CSF as a foundational tool for managing cybersecurity risks and securing critical infrastructure. However, the appendices fail to connect the strategy's initiatives to the five core functions of the NIST CSF: identify, protect, detect, respond, and recover. For instance, while the main strategy discusses the importance of cybersecurity enhancements, the appendices do not provide the operational depth needed to align these initiatives with NIST CSF principles. The absence of clear mappings makes it difficult to assess whether the strategy adequately addresses its compliance obligations.

The lack of specificity is particularly evident in discussions about risk management frameworks and methodologies. NIST SP 800-37 outlines a Risk Management Framework (RMF) that emphasizes a lifecycle approach to identifying, assessing, and mitigating risks. This process includes critical steps such as categorizing information systems, selecting and implementing controls, and conducting continuous monitoring. The appendices, however, do not describe how the DoD will integrate the RMF into its modernization efforts. There is no discussion of how risk categorization will inform decision-making or how monitoring tools will provide real-time visibility into threats. This omission raises concerns about the strategy's ability to operationalize risk management in a manner consistent with EO 13800 and NIST guidelines.

Another critical gap lies in the treatment of supply chain risks. The DoD's reliance on third-party vendors and external providers introduces significant vulnerabilities, particularly as the Department integrates cloud technologies and other advanced systems. NIST SP 800-161 provides detailed guidance on managing supply chain risks, emphasizing the importance of vendor assessments, secure procurement practices, and monitoring the integrity of external components. While the appendices briefly mention supply chain considerations, they do not provide a structured framework for addressing these risks. For example, there is no mention of how vendors will be vetted for compliance with NIST standards or how the DoD will ensure that external dependencies do not introduce vulnerabilities into critical systems. This lack of detail undermines the strategy's ability to safeguard its modernization efforts against supply chain threats.

The appendices also fail to address the need for measurable metrics and accountability mechanisms, a key requirement of EO 13800. The executive order emphasizes the importance of tracking progress in cybersecurity and IT

modernization through quantifiable benchmarks. Metrics such as the percentage of systems compliant with NIST SP 800-53, incident response times, or the adoption rate of zero-trust principles could provide valuable insights into the strategy's effectiveness. However, the appendices do not include any such metrics, leaving a significant gap in the ability to evaluate the strategy's success. Without clear benchmarks, it is difficult to hold stakeholders accountable or ensure that the strategy's goals are being met.

In terms of operational implementation, the appendices lack clarity on how continuous monitoring and incident response will be integrated into the modernization strategy. NIST SP 800-53 and SP 800-171 both emphasize the importance of real-time monitoring to identify and respond to threats. Similarly, EO 13800 mandates robust incident response capabilities to ensure resilience against cyberattacks. The appendices do not detail the tools, processes, or frameworks that will be used to achieve these objectives. For example, there is no mention of how monitoring data will be analyzed, how responses will be coordinated across different teams, or how lessons learned from incidents will inform future practices. This omission represents a critical gap in the strategy's ability to meet federal cybersecurity standards.

Another notable omission is the lack of integration between workforce development and IT modernization. The DoD's ability to execute its modernization strategy depends heavily on the skills and expertise of its personnel. NIST SP 800-53 includes controls for personnel security, emphasizing the need for training and awareness programs tailored to emerging threats and technologies. While the main strategy briefly mentions workforce development, the appendices do not provide details on how these programs will be aligned with the technical requirements of IT modernization. For example, there is no mention of how training will be adapted to address the complexities of zero-trust architectures, cloud technologies, or AI systems. This disconnect between workforce initiatives and modernization efforts could hinder the strategy's effectiveness.

Finally, the appendices miss an opportunity to provide a cohesive roadmap for achieving the strategy's goals. A well-structured roadmap would outline the sequence of initiatives, dependencies, and timelines for implementation. It would also identify key milestones and deliverables, ensuring that all stakeholders are aligned in their efforts. The absence of such a roadmap leaves the strategy without a clear path forward, making it difficult to assess whether its objectives are realistic or achievable.

The Appendices and Supporting Material section of the DoD Digital Modernization Strategy fails to provide the operational depth and technical detail necessary to support the strategy's ambitious goals. The lack of explicit mappings to compliance frameworks such as the NIST CSF and publications like SP 800-53, SP 800-37, SP

800-161, and SP 800-171 represents a significant oversight. Similarly, the absence of measurable metrics, supply chain risk management frameworks, and detailed implementation plans undermines the strategy's alignment with EO 13800. To address these deficiencies, the appendices must be expanded to include direct references to NIST standards, clear benchmarks for success, and structured methodologies for managing risks and ensuring accountability. Without these enhancements, the strategy risks falling short of its stated objectives and failing to meet federal cybersecurity mandates.

The DoD Digital Modernization Strategy 2019 presents a bold and forward-looking framework aimed at overhauling the Department's digital capabilities to maintain technological superiority and safeguard national security. However, when assessed against the stringent requirements of EO 13800 and the principles of the NIST Cybersecurity Framework (NIST CSF), significant gaps emerge, particularly in translating high-level objectives into actionable plans and compliance mechanisms. The strategy's lack of operational depth, explicit mapping to federal mandates, and measurable outcomes compromises its potential to fully meet the expectations set forth by EO 13800 and the NIST SP 800 series standards, including SP 800-53, SP 800-37, SP 800-30, SP 800-161, and SP 800-171.

At its core, EO 13800 calls for agencies to adopt the NIST CSF to enhance cybersecurity resilience and ensure comprehensive risk management across critical infrastructure. The DoD's strategy reflects an alignment in spirit with these objectives, but the absence of explicit references to the five core functions of the NIST CSF—identify, protect, detect, respond, recover—creates ambiguity about its adherence to this foundational framework. Without clear mappings of its initiatives to these functions, the strategy fails to demonstrate how it will achieve the layered, risk-based approach necessary to secure its vast IT ecosystem.

The Foreword and Executive Summary articulate a vision of modernization rooted in innovation, efficiency, and resilience. These are commendable aspirations, but they lack operational clarity. The summary emphasizes zero-trust principles, cloud adoption, and cybersecurity, but it does not outline the processes or controls required to implement these initiatives. For example, zero trust is a cornerstone of modern cybersecurity, yet the strategy does not address how it will manage authentication, micro-segmentation, or secure data flows across the Department's diverse and often legacy-laden systems. These omissions reflect a disconnect between the high-level vision and the practical steps needed to comply with NIST standards like SP 800-207, which outlines zero-trust architectures.

The Goals and Objectives section identifies critical areas of focus, including IT optimization, workforce development, and leveraging data and artificial intelligence (AI). While these objectives are aligned with EO 13800's call for modernization, the

strategy’s lack of metrics or detailed implementation plans undermines its ability to meet federal requirements. For instance, workforce development is essential for managing complex IT systems, yet the strategy does not integrate training initiatives with cybersecurity mandates outlined in SP 800-53, particularly those related to personnel awareness and role-based security. Similarly, while IT optimization is a stated goal, the strategy does not address how modernization efforts will be balanced with interim risk controls for legacy systems, as required by SP 800-30.

The Strategic Elements section—focused on innovation, security, scalability, and interoperability—provides a strong conceptual foundation but lacks the specificity needed to operationalize these principles. Innovation and scalability, while critical for keeping pace with adversaries, introduce significant risks, particularly when untrusted supply chains or untested technologies are involved. NIST SP 800-161 explicitly addresses supply chain risk management, yet the strategy does not detail how these risks will be mitigated during the adoption of new technologies or integration of third-party components. Furthermore, interoperability, while improving efficiency, increases the attack surface, a concern that the strategy does not address with robust access controls, segmentation, or continuous monitoring as prescribed in SP 800-53 and SP 800-37.

The Key Initiatives and Cybersecurity Framework section highlights cloud adoption, AI, and enhanced cybersecurity as central pillars of the modernization effort. These initiatives align with modernization priorities, but their execution lacks alignment with critical federal mandates. Cloud environments, for example, introduce unique risks related to third-party vendors and data protection. While SP 800-171 and SP 800-53 provide clear guidelines for securing cloud-based data, the strategy does not outline how these controls will be implemented or monitored. Similarly, AI systems, which are particularly vulnerable to adversarial manipulation, are not addressed with the level of rigor required by SP 800-53 or SP 800-161, leaving a gap in managing risks associated with emerging technologies.

The IT Modernization and Joint Information Environment (JIE) section emphasizes replacing outdated systems, integrating cloud services, and improving interoperability across the Department. These are necessary steps for achieving operational efficiency, but they come with heightened risks that the strategy does not adequately address. Legacy systems, for instance, are often the weakest link in an IT ecosystem, yet the strategy fails to provide a plan for securing these systems during their transition or decommissioning. EO 13800 and SP 800-30 require robust interim controls and risk assessments for such scenarios, but the strategy’s silence on this front represents a significant oversight. Additionally, the integration of cloud services and interconnected environments expands the attack surface, necessitating continuous monitoring and robust incident response plans. While these are central tenets of SP

800-53 and the NIST CSF, the strategy does not provide detailed plans for implementing these measures.

The Appendices and Supporting Material section should serve as the technical backbone of the strategy, providing the granular details and references needed to support its ambitious goals. However, this section falls short in delivering the specificity required for compliance. The lack of direct references to the NIST CSF and critical publications like SP 800-53, SP 800-37, and SP 800-161 leaves significant gaps in the strategy's alignment with federal mandates. Furthermore, the absence of metrics for evaluating success—such as system uptime, compliance rates, or incident response times—undermines the strategy's ability to demonstrate progress or ensure accountability.

The 2019 DoD Digital Modernization Strategy is not just a failure of strategic foresight; it is a glaring example of willful negligence that borders on intentional disregard for EO 13800 and the federal mandates that were enacted to safeguard national security. Its shortcomings are not mere administrative oversights but systemic breaches of responsibility that jeopardized the nation's defense infrastructure, placing it in clear violation of its constitutional and legal obligations. The DoD's inability—or refusal—to comply with these critical cybersecurity requirements constitutes a failure to uphold its duty to protect the United States from threats, foreign and domestic, both physical and cyber. Viewed through a lens of accountability, this negligence could indeed be construed as intent to undermine national security, raising serious questions of culpability and potential violations of oaths of office.

At its core, EO 13800 is a legal mandate, not a guideline, requiring all federal agencies to adopt the NIST Cybersecurity Framework (NIST CSF) as the foundation for managing cybersecurity risks. This framework is the benchmark for protecting critical infrastructure, demanding explicit integration of the five core functions—Identify, Protect, Detect, Respond, Recover—into every strategy and operational plan. Yet, the DoD's modernization strategy flagrantly disregards this directive. Its failure to explicitly map its initiatives to these functions is not just an oversight; it is a deliberate act of omission that exposed the Department's systems to cyber threats. This abdication of responsibility placed the nation's security in peril, undermining the very foundation of defense against foreign adversaries and domestic vulnerabilities.

The failure to protect Controlled Unclassified Information (CUI) within cloud environments is one of the most egregious examples of this negligence. Federal law, including NIST SP 800-171, mandates stringent controls for safeguarding sensitive data, yet the strategy provides no concrete measures for achieving compliance. This lack of action left critical data exposed, effectively offering adversaries a roadmap to exploit the Department's weaknesses. Similarly, the absence of a structured approach

to managing supply chain risks, as required by NIST SP 800-161, created unmonitored vulnerabilities that adversaries could easily exploit. These failures were not accidental; they stem from a clear decision to prioritize operational convenience over the security protocols required by federal law.

The DoD's neglect in establishing robust incident response and recovery plans compounds the severity of its failures. EO 13800 explicitly requires agencies to prepare for and recover from cyber incidents, yet the strategy lacks any substantive framework for addressing these critical functions. In an era of escalating cyberattacks, this failure to prepare is tantamount to leaving the nation's defense systems undefended. Without tested incident response plans, the Department is unable to mitigate damage from breaches, recover operations effectively, or learn from attacks to improve future defenses. This negligence directly contravenes the Respond and Recover functions of the NIST CSF and violates the explicit requirements of EO 13800.

The lack of measurable metrics and accountability mechanisms further highlights the Department's disregard for its obligations. EO 13800 demands quantifiable outcomes to evaluate progress in enhancing cybersecurity resilience. The strategy's focus on operational milestones, such as the number of cloud migrations or DevSecOps pipelines implemented, ignores critical measures like incident response times, vulnerability reduction, or compliance rates with NIST SP 800-53. This failure to track meaningful outcomes obfuscates the strategy's effectiveness, allowing systemic vulnerabilities to persist unchecked. It is not just a failure of execution but a deliberate choice to avoid accountability for safeguarding the nation's critical systems.

These failures are not just administrative missteps; they are clear violations of the DoD's oath to defend the United States against all threats, foreign and domestic. Cybersecurity is as much a part of national defense as physical barriers or military readiness. The Department's negligence in adhering to EO 13800's mandates undermined its ability to protect the nation from increasingly sophisticated cyber adversaries. This failure to act with due diligence in securing critical infrastructure is not just a dereliction of duty but a betrayal of the trust placed in the Department to protect the American people.

When viewed through the lens of legal accountability, the DoD's actions—or inactions—could be interpreted as willful intent. By ignoring federal mandates and failing to implement basic cybersecurity protections, the Department knowingly placed the nation's security at risk. This pattern of negligence aligns with the legal principle of "reckless disregard," which suggests an awareness of the consequences but a deliberate choice to ignore them. In the context of national security, such actions could be construed as violations of federal law and potentially rise to the level

of treason. The deliberate neglect of EO 13800's requirements undermines the ability of the United States to defend itself in the cyber domain, effectively aiding adversaries by leaving critical vulnerabilities exposed.

Moreover, this negligence represents a breach of the solemn oath taken by DoD leadership to uphold and defend the Constitution. This oath is not symbolic; it binds every official to a standard of action that ensures the safety and security of the nation. By failing to defend against cyber threats as EO 13800 demands, the Department violated this oath, betraying its responsibility to "we the people." Such breaches erode public trust and weaken the nation's ability to project strength and resilience in the face of evolving threats.

The consequences of these failures are not theoretical; they are unfolding in real time. The same systemic lapses identified in the 2019 strategy persist today, leaving the United States vulnerable to cyberattacks that target critical infrastructure, steal sensitive data, and disrupt national security operations. This continuity of negligence underscores the urgent need for accountability and reform. Without immediate action to address these deficiencies, the nation remains exposed to adversaries who exploit every weakness to undermine its security and stability.

In conclusion, the 2019 DoD Digital Modernization Strategy is a stark example of willful negligence that violated EO 13800, federal law, and the sacred oaths of office sworn by Department leadership. Its failures to align with federal mandates and protect critical systems constitute a clear and present danger to the United States. This strategy is more than a missed opportunity; it is a betrayal of the nation's trust and a breach of the fundamental responsibilities of national defense. The Department of Defense must be held accountable for these failings and take immediate, decisive action to close the gaps that continue to jeopardize the security of the United States.

DoD-Digital-Modernization-Strategy-2019.pdf - https://docdro.id/8Kyrprl

DoD Software Modernization Strategy (2022)

The DoD Software Modernization Strategy (2022) outlines a vision for enhancing the Department's software development capabilities, emphasizing speed, security, and innovation. Its focus on DevSecOps, cloud-native environments, and artificial intelligence (AI) reflects the DoD's commitment to keeping pace with technological advancements. However, when examined against the requirements of EO 13800 and the NIST Cybersecurity Framework (NIST CSF), the strategy reveals a mix of alignment and gaps that require deeper exploration.

At its core, the strategy aims to accelerate software delivery while embedding security into every phase of the development lifecycle. This commitment to DevSecOps is a significant step forward, aligning conceptually with the Protect and Detect functions of the NIST CSF. Automation, testing, and continuous monitoring are emphasized as pillars of secure development pipelines, suggesting an effort to integrate security seamlessly into operations. Yet, the strategy falls short in detailing how these DevSecOps environments will comply with the rigorous standards of NIST SP 800-53 and SP 800-171, particularly in protecting Controlled Unclassified Information (CUI). The absence of specifics on access controls, vulnerability management, and incident response measures leaves critical compliance questions unanswered.

Cloud adoption is another cornerstone of the strategy, promising scalability and efficiency. Transitioning to cloud-native architectures is aligned with EO 13800's mandate to modernize federal IT infrastructure. However, cloud environments inherently introduce new risks, particularly in securing sensitive data and managing third-party dependencies. While the strategy discusses enterprise cloud adoption, it does not address how compliance with SP 800-171 requirements for data protection will be achieved. Similarly, NIST SP 800-161 highlights the importance of supply chain risk management, yet the strategy does not outline processes for vetting cloud service providers or ensuring their security measures meet federal standards. This lack of a structured approach to managing cloud-related risks undermines the strategy's alignment with EO 13800.

The strategy's emphasis on AI and machine learning (ML) is forward-thinking, recognizing these technologies as critical to maintaining a technological edge. However, AI and ML systems come with unique vulnerabilities that require proactive risk management. Adversarial manipulation, data poisoning, and biases in training models are well-documented threats, but the strategy does not address these challenges in detail. NIST SP 800-53 and SP 800-161 provide guidelines for securing data inputs and protecting the integrity of AI systems, yet the strategy lacks explicit measures for implementing these controls. Without a clear framework for managing AI-specific risks, the DoD risks introducing vulnerabilities into its operations.

Measurable progress is a recurring theme in EO 13800, which emphasizes the need for clear metrics to evaluate the effectiveness of cybersecurity initiatives. The strategy mentions general milestones, such as increasing DevSecOps adoption and expanding cloud capabilities, but it does not define specific benchmarks. Metrics such as incident response times, compliance rates with SP 800-53, or the reduction in vulnerabilities across development pipelines would provide tangible indicators of success. The absence of these metrics makes it difficult to assess whether the strategy is achieving its goals or aligning with federal mandates.

The strategy also lacks explicit references to the five core functions of the NIST CSF—Identify, Protect, Detect, Respond, Recover. While its focus on DevSecOps and continuous delivery aligns broadly with the Protect and Detect functions, other areas are underdeveloped. The Identify function, which involves asset inventory and risk assessment, is mentioned only in passing. Plans for implementing the Respond and Recover functions, critical for incident response and resilience, are notably absent. This lack of alignment with the NIST CSF leaves gaps in the strategy's ability to address cybersecurity comprehensively.

Supply chain risks are another area of concern. The strategy's focus on agility and innovation is commendable, but it must be balanced with robust controls to manage third-party dependencies. NIST SP 800-161 provides detailed guidance on evaluating and mitigating supply chain risks, yet the strategy does not incorporate these recommendations. For example, there is no mention of how the DoD will assess the security of vendors contributing to DevSecOps pipelines or cloud services. This omission is particularly concerning given the increasing prevalence of supply chain attacks targeting software development environments.

Incident response and recovery are critical components of any cybersecurity strategy, particularly for an organization as complex and targeted as the DoD. While the strategy emphasizes resilience, it does not provide actionable plans for responding to or recovering from cyber incidents. NIST SP 800-53 and the NIST CSF emphasize the importance of regular testing, tabletop exercises, and post-incident evaluations to ensure readiness. The absence of these measures in the strategy represents a significant gap, leaving the DoD potentially unprepared to address evolving threats.

The strategy's overarching focus on innovation, speed, and security is well-intentioned, but its lack of operational detail and explicit compliance measures undermines its ability to meet the mandates of EO 13800. To address these gaps, the strategy must explicitly incorporate the requirements of the NIST CSF and related publications, providing detailed implementation plans, metrics for progress, and accountability mechanisms. Without these enhancements, the strategy risks falling short of its stated objectives and leaving critical vulnerabilities unaddressed.

The 2022 DoD Software Modernization Strategy represents yet another missed opportunity for the Department of Defense to align its modernization efforts with the mandates of EO 13800 and to address the cybersecurity vulnerabilities that continue to plague our nation's defense infrastructure. Over three years after the 2019 Digital Modernization Strategy, this document should have been a corrective step—a chance to close the glaring compliance gaps and secure the Department against escalating cyber threats. Instead, it demonstrates a continued pattern of willful neglect, incompetence, and disregard for the legal and constitutional obligations entrusted to the DoD by the American people. This failure transcends administrations and

secretaries of defense, revealing a systemic issue that leaves the United States exposed to cyberattacks, now as much as in 2019.

Despite a new administration and a changing leadership structure at the DoD, the 2022 strategy is devoid of any meaningful reference to EO 13800 or the NIST Cybersecurity Framework (NIST CSF)—the very federal standards designed to guide critical infrastructure protection. This omission cannot be seen as anything other than negligence or intentional defiance. EO 13800 is not advisory; it is a legal mandate requiring federal agencies to adopt the NIST CSF and align their cybersecurity practices with its core functions: Identify, Protect, Detect, Respond, and Recover. For the DoD to continue ignoring these fundamental principles, year after year, suggests either a profound misunderstanding of the law or a deliberate decision to sidestep it.

This strategy's failure to prioritize compliance with NIST SP 800-53, SP 800-37, SP 800-171, and SP 800-161 further exacerbates its inadequacy. These standards are the bedrock of federal cybersecurity, providing clear, actionable controls for protecting sensitive information, managing risks, and ensuring resilience. Yet the 2022 strategy offers no evidence that its initiatives—such as DevSecOps pipelines, enterprise cloud adoption, or AI integration—adhere to these critical requirements. For example, it speaks broadly about securing software development lifecycles but fails to outline how Controlled Unclassified Information (CUI) will be safeguarded under SP 800-171. Similarly, it champions cloud scalability without addressing the supply chain risks that are explicitly covered in SP 800-161. These omissions are not minor oversights; they represent a complete failure to meet the cybersecurity obligations imposed by federal law.

The absence of concrete plans for incident response and recovery remains another glaring flaw in the 2022 strategy. Cyber incidents are no longer hypothetical scenarios—they are daily realities that threaten the very fabric of national security. Yet, the strategy provides no detailed framework for responding to breaches, mitigating damage, or restoring operations in the aftermath of an attack. The lack of focus on the Respond and Recover functions of the NIST CSF is a dereliction of duty that leaves the Department unprepared to handle the inevitable. This negligence not only violates EO 13800 but also endangers the lives of Americans by failing to ensure the resilience of critical defense systems.

The persistent absence of measurable metrics and accountability mechanisms underscores a broader culture of irresponsibility within the DoD. The strategy's milestones are vague and operationally focused—such as increasing the number of DevSecOps pipelines or migrating systems to the cloud—but fail to track the metrics that matter: reductions in vulnerabilities, faster incident response times, or improved compliance with federal standards. Without these benchmarks, the DoD's progress is impossible to evaluate, creating a dangerous lack of transparency and accountability.

EO 13800 explicitly demands measurable outcomes to ensure cybersecurity resilience, yet the 2022 strategy flagrantly ignores this requirement, perpetuating the same culture of avoidance and obfuscation seen in 2019.

What is perhaps most damning is that this continued negligence spans multiple administrations and secretaries of defense. This is not a partisan issue, nor is it the failure of any single individual. It reflects a systemic disregard for cybersecurity within the Department, suggesting that leadership at the highest levels has either failed to grasp the severity of the threat or has chosen to ignore it altogether. This failure to act, even in the face of increasing cyberattacks, suggests a willful neglect of duty. If leadership has not read EO 13800, the NIST CSF, or the federal standards they are obligated to uphold, it is not only a failure of competence but also a breach of their sworn oaths to protect the nation. If they have read these mandates and chosen to ignore them, the situation is even more dire, as it implies deliberate intent to sidestep the very laws designed to secure our nation.

The result of this failure is a DoD that remains unprotected against escalating cyber threats, leaving the nation vulnerable to attacks that could compromise critical infrastructure, steal sensitive defense data, and disrupt national security operations. These lapses have a cascading effect, weakening public trust, emboldening adversaries, and undermining the nation's ability to project strength in an increasingly volatile global landscape. The lack of compliance with EO 13800 and the NIST CSF is not just a technical deficiency—it is a breach of trust and a betrayal of the American people, who rely on the Department to safeguard the nation against all threats, physical and cyber.

This ongoing failure raises serious questions about intent. The repeated refusal to comply with federal mandates, despite years of opportunity to correct course, suggests more than incompetence—it suggests a deliberate choice to sideline cybersecurity in favor of other priorities. In the context of national security, this negligence could be construed as aiding and abetting adversaries by leaving critical systems vulnerable to attack. Such willful disregard for the nation's security obligations violates not only EO 13800 but also the constitutional duty of the Department's leadership to protect the United States. It is a dereliction of duty so severe that it borders on treason, as it knowingly compromises the safety and sovereignty of the nation.

The 2022 DoD Software Modernization Strategy is not a solution—it is a symptom of a systemic problem that has persisted for far too long. It reflects a Department unwilling or unable to rise to the challenges of the modern cyber threat landscape, ignoring the very standards that were created to protect it. The continued failure to comply with EO 13800, across multiple administrations and leadership changes, is a stark reminder that the DoD's cybersecurity failures are not isolated incidents but

institutional failures. The stakes could not be higher, and the cost of inaction is measured not just in systems compromised or data stolen but in the erosion of national security itself. The DoD must face accountability for these failures, and immediate, decisive action is required to rectify the systemic neglect that endangers the nation's future.

Department-Of-Defense-Software-Modernization-Strategy.pdf
https://docdro.id/4pnhc7s

DoD Software Modernization Implementation Plan (2023)

The DoD Software Modernization Implementation Plan (2023) provides a structured roadmap for implementing the objectives outlined in the 2022 Software Modernization Strategy. It emphasizes milestones, timelines, and specific actions to drive the adoption of modern software development practices, enterprise cloud capabilities, and streamlined acquisition processes. While this plan represents a significant advancement in operationalizing the DoD's modernization goals, a closer examination against EO 13800 and the NIST Cybersecurity Framework (NIST CSF) highlights notable areas of alignment and critical gaps.

At its heart, the plan prioritizes expanding the use of DevSecOps practices. This focus reflects the Department's commitment to embedding security at every stage of the software development lifecycle. DevSecOps' emphasis on automation, continuous integration, and real-time monitoring aligns conceptually with the Protect and Detect functions of the NIST CSF. However, the implementation plan lacks explicit details on how these pipelines will comply with the rigorous security controls outlined in NIST SP 800-53, particularly those related to the protection of Controlled Unclassified Information (CUI). Questions about encryption standards, access management, and vulnerability detection remain unanswered. For instance, while the plan underscores the importance of secure pipelines, it does not clarify the specific measures to ensure that software environments meet federal cybersecurity requirements. This omission creates a gap in demonstrating how DevSecOps practices will align with EO 13800's risk management mandates.

The push for enterprise cloud modernization is another focal point of the plan. Cloud environments offer scalability and efficiency, making them essential for supporting modern software practices. The plan recognizes this but does not address the security challenges inherent in cloud adoption. NIST SP 800-171 and SP 800-53 provide robust guidance for protecting data in cloud environments, yet the plan fails to detail how these standards will be applied. While the plan discusses partnerships with cloud vendors, it lacks a framework for evaluating vendor security or managing third-party

risks, both critical components of NIST SP 800-161. Without clear processes for securing data and ensuring vendor compliance, the reliance on cloud services introduces vulnerabilities that could undermine mission-critical operations.

One of the plan's strengths is its focus on streamlining software acquisition and deployment. Rapid prototyping and iterative development are emphasized as ways to accelerate the delivery of software capabilities. These initiatives align with EO 13800's modernization objectives but carry inherent risks if not managed carefully. The plan does not describe how software acquisition processes will incorporate the risk assessments and security controls required by NIST SP 800-53 and SP 800-37. For example, will vendors be required to demonstrate compliance with NIST standards before procurement? How will the DoD ensure that acquired software is free from vulnerabilities before deployment? The lack of clarity on these points raises concerns about the potential introduction of unverified or insecure software into the Department's ecosystem.

The plan's emphasis on metrics and accountability is a welcome addition, providing specific milestones and timelines for measuring progress. These include the number of operational DevSecOps pipelines and the percentage of systems migrated to enterprise cloud environments. While these metrics enhance transparency and progress tracking, they are primarily focused on operational outputs rather than cybersecurity outcomes. EO 13800 emphasizes the need for measurable progress in improving cybersecurity resilience, but the plan does not include metrics for evaluating incident response times, vulnerability reduction, or compliance rates with NIST SP 800-53 and SP 800-171. Without such metrics, it is challenging to assess the plan's effectiveness in enhancing the DoD's cybersecurity posture.

The Respond and Recover functions of the NIST CSF are particularly underdeveloped in the plan. Cloud services and interconnected software environments increase the likelihood of cyber incidents, yet the plan does not provide detailed measures for incident response or recovery. Regular testing of incident response capabilities, as outlined in NIST SP 800-53, is essential for ensuring readiness, but the plan does not address how these exercises will be conducted. Similarly, recovery strategies for restoring mission-critical operations after a cyberattack are absent, leaving a critical gap in the plan's ability to address EO 13800's resilience requirements.

Supply chain risks are briefly mentioned but insufficiently addressed. The reliance on third-party software and cloud vendors introduces vulnerabilities that could be exploited by adversaries. NIST SP 800-161 provides comprehensive guidance on managing supply chain risks, emphasizing vendor assessments, secure procurement practices, and monitoring for supply chain attacks. The plan acknowledges these risks but does not provide a structured approach to mitigating them. For example, there is

no mention of how vendors will be evaluated for compliance or how supply chain vulnerabilities will be monitored and addressed. This omission is particularly concerning given the increasing prevalence of supply chain attacks targeting software development ecosystems.

The implementation plan builds upon the foundations of the 2022 Software Modernization Strategy, adding much-needed structure and accountability to the DoD's modernization efforts. However, its focus on operational milestones without corresponding cybersecurity measures leaves significant gaps. The plan's emphasis on rapid software delivery, cloud adoption, and acquisition reform is commendable, but it must be accompanied by robust risk management practices and alignment with federal mandates to ensure success.

The DoD Software Modernization Implementation Plan (2023) exposes critical vulnerabilities that represent a significant national security threat and highlight potential violations of federal law and established national security protocols. While the plan's intent to modernize software capabilities is clear, its execution leaves the nation's defense infrastructure exposed to systemic risks that could be exploited by adversaries. The absence of robust controls, detailed risk management frameworks, and explicit compliance with EO 13800 and the NIST Cybersecurity Framework (NIST CSF) underscores a failure to meet federally mandated standards designed to safeguard critical systems.

The plan's treatment of DevSecOps, enterprise cloud environments, and acquisition reform is superficial, prioritizing operational speed and efficiency over the security measures essential for protecting mission-critical systems. By not detailing encryption standards, access controls, or continuous monitoring practices, the plan fails to align with the requirements of NIST SP 800-53 and SP 800-171, leaving sensitive data, including Controlled Unclassified Information (CUI), exposed. This is a clear breach of federal cybersecurity requirements and places the integrity of the DoD's operations at risk.

The reliance on cloud vendors and third-party software providers without a structured framework for managing supply chain risks further exacerbates this threat. NIST SP 800-161 mandates rigorous evaluation and monitoring of vendors to prevent the introduction of vulnerabilities into critical systems. The plan's failure to address these risks comprehensively not only undermines federal compliance but also creates a pathway for adversaries to exploit supply chain weaknesses. In an era of increasing cyberattacks targeting supply chains, this oversight is a glaring lapse in national security responsibility.

Additionally, the lack of focus on incident response and recovery capabilities leaves the Department unprepared to mitigate or recover from cyberattacks. The absence of

concrete plans for responding to breaches or restoring operations following an attack represents a fundamental failure to adhere to the Respond and Recover functions of the NIST CSF. This omission could have catastrophic consequences in the event of a large-scale cyberattack, potentially crippling the DoD's ability to operate effectively during a national emergency or conflict.

Perhaps most alarming is the lack of measurable metrics to assess the effectiveness of the modernization efforts in improving cybersecurity resilience. EO 13800 explicitly requires agencies to demonstrate progress in securing their systems, yet the plan focuses on operational outputs like the number of DevSecOps pipelines or cloud migrations, ignoring critical indicators such as reduced vulnerabilities, faster incident response times, or compliance rates with NIST standards. This lack of accountability and transparency raises serious questions about whether the DoD is meeting its obligations to protect national security.

The weaknesses outlined in this plan are not merely procedural oversights; they represent a dereliction of duty in adhering to federally mandated standards that are critical for safeguarding the nation's defense infrastructure. By failing to implement comprehensive risk management practices, secure its software ecosystems, and prepare for cyber incidents, the DoD risks exposing its operations to adversaries, endangering national security and violating the principles outlined in EO 13800. These failures must be recognized as urgent national security threats that demand immediate attention and remediation.

If the deficiencies in this implementation plan are not addressed, the consequences could extend beyond the Department of Defense, potentially destabilizing critical national infrastructure and compromising the United States' ability to defend itself against both physical and cyber threats. This document stands as a stark warning of the vulnerabilities that must be urgently rectified to secure the nation's future.

DoD Approves Software Modernization Implementation Plan_U.S. Department of Defense_Release.pdf
https://docdro.id/udfHNHs%0A

DoD Cyber Strategy Summary (2023)

The 2023 DoD Cyber Strategy Summary offers a glimpse into the Department of Defense's evolving approach to cybersecurity amid an increasingly complex global threat landscape. While the document reflects some recognition of the need for innovation, partnerships, and resilience, it remains insufficiently detailed to address the foundational requirements of EO 13800 and the NIST Cybersecurity Framework (NIST CSF). The strategy's gaps in compliance and actionable specifics undermine its potential, perpetuating vulnerabilities that adversaries are well-positioned to

exploit. In its current form, the strategy appears more aspirational than operational, leaving critical areas of national defense exposed to significant risks.

The strategy's emphasis on partnerships represents one of its most promising elements. By highlighting the importance of collaboration with allies, private sector stakeholders, and interagency partners, the DoD acknowledges that cybersecurity is a shared responsibility. This shift toward cooperative defense marks an improvement over earlier strategies, which often focused solely on internal modernization. However, the effectiveness of these partnerships depends on their execution. The strategy fails to specify how these relationships will be operationalized or how partner organizations will be held to the same rigorous cybersecurity standards required by NIST SP 800-161. Without clear processes for evaluating the security practices of vendors and allies, these partnerships risk introducing additional vulnerabilities into the Department's ecosystem. A structured framework for managing third-party risks, including regular audits and transparent compliance requirements, is essential for turning these partnerships into a strength rather than a liability.

Another notable aspect of the strategy is its focus on proactive defense through emerging technologies such as artificial intelligence (AI) and advanced analytics. This approach demonstrates an understanding of the need to anticipate and mitigate cyber threats before they materialize. However, the implementation of AI introduces unique risks that are not adequately addressed in the strategy. AI systems are inherently vulnerable to adversarial manipulation, data poisoning, and algorithmic exploitation. The lack of comprehensive safeguards for securing AI ecosystems—such as protecting training data and algorithms—leaves these systems open to exploitation. Federal standards like NIST SP 800-53 outline the necessary controls for securing such technologies, but the strategy offers no indication that these measures will be implemented. To fully leverage AI's potential, the Department must prioritize the development of robust monitoring systems and fail-safes that ensure the integrity and reliability of these tools.

The strategy's treatment of resilience is another area where it falls short. While the document frequently references the importance of resilience, it provides no actionable details on how the Department will achieve it. The Respond and Recover functions of the NIST CSF are critical for ensuring that organizations can quickly contain and recover from cyber incidents, yet the strategy offers little beyond vague commitments. EO 13800 mandates that federal agencies develop and test comprehensive incident response protocols, including detailed procedures for detecting, containing, and mitigating breaches. The strategy's failure to outline these steps leaves the DoD unprepared to handle the inevitable reality of cyber incidents. Regular red-teaming exercises, tabletop simulations, and secure, off-site backups of critical systems are essential components of resilience that must be incorporated into

the strategy. Without these measures, the Department remains at risk of prolonged disruptions and operational paralysis in the wake of a significant attack.

The strategy's focus on cloud adoption highlights the Department's recognition of the scalability and efficiency that cloud technologies can offer. However, cloud environments are inherently complex and introduce significant cybersecurity challenges. Federal standards like NIST SP 800-171 and SP 800-53 require robust encryption, identity and access management (IAM), and continuous monitoring for all cloud systems. The strategy's failure to specify how these controls will be implemented undermines its credibility. Additionally, the document neglects to address the unique risks associated with third-party cloud vendors, a recurring weakness in the Department's cybersecurity posture. The absence of vendor compliance requirements and regular security audits leaves critical data and systems exposed to supply chain vulnerabilities.

Legacy systems continue to represent a critical vulnerability, yet the strategy provides no roadmap for their assessment, modernization, or phased replacement. These outdated systems, often operating on obsolete software, present known risks that adversaries are well-equipped to exploit. Federal standards like NIST SP 800-30 and SP 800-37 provide clear guidance for managing the risks associated with legacy systems, including conducting risk assessments, implementing interim protections, and developing phased migration plans. The strategy's failure to address these requirements perpetuates a significant weakness in the Department's defenses.

The emphasis on workforce development reflects an understanding of the human element in cybersecurity, but the strategy lacks the depth needed to address this critical area. While the document highlights the need for skilled personnel, it does not provide a detailed plan for recruiting, training, or retaining cybersecurity talent. Certifications in DevSecOps, cloud security, and AI risk management should be mandatory for relevant roles, and competitive compensation must be offered to attract and retain top talent. A robust workforce development program, aligned with NIST SP 800-53, is essential for ensuring that the Department has the expertise needed to implement its cybersecurity initiatives effectively.

Conclusion

The 2023 DoD Cyber Strategy Summary reflects a growing awareness of the need to address the complex challenges of modern cybersecurity, but its lack of actionable specifics undermines its potential. While the emphasis on partnerships and proactive defense represents progress, these elements are insufficient without the structural and operational frameworks required to support them. The strategy's failure to align with EO 13800 and the NIST Cybersecurity Framework continues a pattern of systemic negligence that leaves the Department vulnerable to escalating cyber threats.

The implications of these shortcomings are profound. By failing to prioritize compliance with federal cybersecurity standards, the strategy perpetuates the vulnerabilities that adversaries have exploited for years. The lack of concrete plans for incident response, cloud security, legacy system modernization, and workforce development reflects an inability—or unwillingness—to address the foundational issues that jeopardize the Department's cybersecurity posture. Without immediate and decisive action to close these gaps, the DoD risks leaving itself unprepared for the challenges of the digital age, compromising national security and undermining public trust.

The 2023 DoD Cyber Strategy Summary serves as the latest in a series of documents purportedly addressing the cybersecurity challenges facing the Department of Defense. Yet, like its predecessors, this strategy fails to meet the fundamental requirements of EO 13800 and the NIST Cybersecurity Framework (NIST CSF), laws and standards designed explicitly to safeguard the nation's critical infrastructure from the escalating cyber threats of today's digital age. Despite the grave importance of cybersecurity in national defense, the DoD's consistent inability—or unwillingness—to comply with these mandates constitutes a dangerous dereliction of duty. This pattern of neglect, spanning multiple strategies and leadership transitions, raises serious questions about whether these failures stem from incompetence or something far more concerning: willful intent to disregard federal law and national security obligations.

EO 13800, signed into law to ensure the protection of federal networks and critical infrastructure, explicitly requires agencies like the DoD to adopt the NIST CSF. This framework is built on five essential functions—Identify, Protect, Detect, Respond, and Recover—which together form a comprehensive roadmap for managing cybersecurity risks. The NIST CSF is not a guideline or suggestion; it is a legal mandate aimed at ensuring that federal agencies are resilient in the face of cyber threats. Yet, despite the existence of multiple documents addressing modernization, strategy, and implementation, the DoD has consistently failed to align its plans with these core functions. This omission is not merely a technical oversight but a violation of federal law and a betrayal of the Department's responsibility to protect the United States from all threats, foreign and domestic.

The 2023 Cyber Strategy Summary reflects the same systemic weaknesses present in the 2019 Digital Modernization Strategy, the 2022 Software Modernization Strategy, and the 2023 Software Modernization Implementation Plan. Across these documents, there is a conspicuous absence of explicit references to EO 13800 and the NIST CSF, as well as the specific federal standards designed to operationalize these mandates, such as NIST SP 800-53, SP 800-171, SP 800-161, SP 800-30, and SP 800-37. These standards provide detailed, actionable frameworks for securing critical infrastructure, managing risks, and ensuring resilience, yet they remain ignored in the Department's

strategic planning. This persistent failure to comply is not a matter of outdated guidance or shifting priorities; it is a willful neglect of the laws and standards enacted to protect the nation.

The implications of this negligence are staggering. The DoD oversees some of the most sensitive and critical systems in the federal government, systems that adversaries are actively targeting to undermine national security. By failing to implement the controls required by EO 13800 and the NIST CSF, the Department has left itself and, by extension, the nation vulnerable to cyberattacks that could cripple defense operations, compromise classified data, and erode public trust. The lack of explicit incident response and recovery protocols, inadequate cloud and supply chain security measures, and failure to address legacy system vulnerabilities demonstrate an unacceptable level of risk for an agency charged with safeguarding the United States. These vulnerabilities are not theoretical; they are actively exploited by adversaries, and the DoD's inaction only emboldens those seeking to harm the nation.

The systemic nature of these failures raises serious questions about intent. A one-time oversight might be excused as incompetence, but a repeated pattern of neglect across multiple strategies and administrations suggests something far more insidious. The refusal to prioritize compliance with EO 13800, even after years of escalating cyberattacks and public scrutiny, borders on willful negligence. This negligence, in the context of national security, could easily be construed as intent. By knowingly leaving critical systems exposed to attack, the Department is effectively aiding and abetting adversaries, whether by omission or design. Such actions—or inactions—undermine the constitutional duty of the Department's leadership to protect the United States and its citizens from threats, both foreign and domestic.

Furthermore, this neglect is a direct violation of the oaths of office taken by those in leadership positions within the DoD. The Secretary of Defense and other senior officials swear to defend the nation against all enemies, yet their repeated failure to comply with federal cybersecurity mandates calls into question their commitment to that oath. Cybersecurity is no longer a secondary concern or administrative burden; it is a frontline defense against adversaries who seek to destabilize the nation. By disregarding the laws and standards that govern this critical domain, the Department's leadership has abdicated its responsibility to protect the United States, potentially jeopardizing the lives of its citizens and the integrity of its defense infrastructure.

The consequences of this negligence are far-reaching. Beyond the immediate risks to national security, the Department's failure to act undermines the credibility of the United States on the global stage. If the DoD cannot secure its own systems, how can it expect to lead in establishing international norms for cybersecurity or rally allies to defend against common threats? This failure erodes trust not only within the United

States but also among its global partners, weakening the nation's ability to project strength and resilience in an increasingly volatile world.

To allow these lapses to continue unchecked is to invite disaster. Cybersecurity threats are no longer hypothetical; they are active, evolving, and capable of inflicting catastrophic damage. The Department of Defense, as the nation's foremost protector against external threats, must set the standard for compliance and resilience. Anything less is a betrayal of its mission and a dereliction of its duty to the American people. The continued refusal to align with EO 13800 and the NIST CSF is more than a legal violation; it is a failure of leadership, a breach of trust, and, potentially, an act of treason against the principles of national security.

The DoD must immediately address these failures by committing to full compliance with EO 13800 and the NIST CSF. This includes developing and implementing comprehensive incident response and recovery protocols, enforcing strict controls for cloud and supply chain security, modernizing legacy systems, and investing in workforce development to build the expertise needed to secure its operations. The Department must also establish clear accountability mechanisms, ensuring that progress is tracked, audited, and transparently reported to the American people. These steps are not optional; they are essential to fulfilling the DoD's constitutional and ethical obligations.

In conclusion, the 2023 DoD Cyber Strategy Summary and its predecessors reflect a systemic failure to prioritize cybersecurity in alignment with federal law and national security protocols. This persistent neglect jeopardizes the safety and sovereignty of the United States, leaving the nation vulnerable to adversaries who exploit these weaknesses with impunity. The Department must take immediate, decisive action to correct these failures, or risk perpetuating a cycle of negligence that endangers the future of the United States and its people.

2023_DOD_Cyber_Strategy_Summary.pdf
https://docdro.id/PcU8KqZ%0A

OSD IT Digital Modernization Roadmap FY2026-2030

The OSD IT Digital Modernization Roadmap FY2026-2030 lays out a vision for the Department of Defense's IT future, focusing on innovative technologies like enterprise cloud adoption, artificial intelligence (AI), and data-driven decision-making. However, this vision is critically undermined by its persistent failure to comply with the requirements of EO 13800 and established federal cybersecurity standards. This roadmap, like its predecessors, demonstrates an ongoing inability—or unwillingness—to address the systemic vulnerabilities that threaten the nation's

security. These deficiencies are not merely technical gaps but violations of the Department's fundamental responsibility to protect the United States from cyber threats, both foreign and domestic.

At the core of these failures is the roadmap's refusal to explicitly align its initiatives with the NIST Cybersecurity Framework (NIST CSF). The NIST CSF provides the foundational structure for managing cybersecurity risks, emphasizing five core functions: Identify, Protect, Detect, Respond, and Recover. These functions are not optional—they are legally mandated under EO 13800 and serve as the backbone of any comprehensive cybersecurity strategy. Yet, the roadmap fails to map its goals and initiatives to these functions. Without this alignment, the Department lacks a cohesive approach to identifying vulnerabilities, protecting critical systems, detecting and mitigating threats, responding to incidents, and recovering from attacks. This failure to integrate such fundamental principles is not only negligent but also a direct violation of federal law.

One of the roadmap's primary focuses is the expansion of enterprise cloud capabilities. While the plan touts the benefits of scalability and efficiency, it provides little assurance that cloud environments will be secured in compliance with federal standards. Both NIST SP 800-53 and SP 800-171 outline stringent requirements for protecting sensitive data in cloud systems, including robust encryption, access controls, and real-time monitoring. Yet the roadmap remains silent on how these measures will be implemented. Even more troubling is the absence of a structured approach to managing third-party cloud vendors, a critical vulnerability that has been exploited in numerous supply chain attacks. The roadmap should have provided clear requirements for vendor compliance, regular security audits, and continuous monitoring, as outlined in NIST SP 800-161. Instead, it leaves these crucial responsibilities unaddressed, perpetuating a glaring weakness in the Department's cybersecurity posture.

The emphasis on AI integration is similarly forward-looking but deeply flawed in execution. AI systems introduce unique risks, including adversarial manipulation, data poisoning, and algorithmic exploitation. Federal standards demand that these risks be managed through rigorous security controls, yet the roadmap fails to address how these controls will be applied. The integrity of training data, the security of algorithms, and the implementation of robust monitoring systems are critical to ensuring that AI enhances rather than undermines national security. By neglecting these safeguards, the roadmap exposes the Department to potential exploitation of its AI systems, turning a technological advantage into a strategic vulnerability.

Incident response and recovery remain critical gaps in the roadmap. While it frequently references resilience, it does not provide actionable details on how the Department will prepare for and respond to cyber incidents. The absence of detailed

protocols, regular testing, and clearly defined recovery strategies reflects a fundamental failure to comply with the Respond and Recover functions of the NIST CSF. These omissions leave the Department unprepared for the inevitable reality of cyberattacks, jeopardizing its ability to restore operations, protect sensitive data, and maintain mission readiness during and after an incident.

The roadmap's approach to metrics and accountability also falls short. While it sets broad milestones for operational objectives like cloud migration and AI adoption, it fails to establish measurable cybersecurity outcomes. EO 13800 explicitly requires that progress be tracked using quantifiable metrics, such as reductions in vulnerabilities, incident response times, and compliance rates with NIST standards. By focusing solely on operational goals, the roadmap obscures the true state of the Department's cybersecurity resilience, making it impossible to assess whether these initiatives are mitigating risks or merely expanding vulnerabilities.

The neglect of legacy systems further highlights the roadmap's inadequacy. These systems are often the weakest link in the Department's infrastructure, yet the roadmap fails to provide a clear strategy for managing their transition to modern platforms. Comprehensive risk assessments, interim protections, and phased migration plans are essential for securing legacy systems during modernization, as outlined in NIST SP 800-30 and SP 800-37. The failure to address these needs leaves critical vulnerabilities unpatched and accessible to adversaries, who are well-versed in exploiting outdated technologies.

Finally, the roadmap does little to address the critical issue of workforce development. Cybersecurity is a human-driven effort, requiring skilled personnel who are trained to recognize and mitigate threats in real time. While the roadmap acknowledges the importance of talent development, it does not provide a detailed plan for equipping the workforce with the skills necessary to implement and maintain these modernization efforts. Certifications in areas like DevSecOps, cloud security, and AI risk management should be mandatory, and competitive compensation packages should be offered to retain top talent. Without a robust workforce development initiative, the Department's ability to execute its roadmap effectively will remain severely compromised.

The OSD IT Digital Modernization Roadmap FY2026-2030 is emblematic of the systemic failures that have plagued the Department's cybersecurity efforts for years. Its ambitious vision for the future is undermined by its refusal to address the foundational requirements of EO 13800 and the NIST CSF. The absence of clear frameworks, actionable plans, and accountability mechanisms perpetuates the same vulnerabilities that have been exploited in the past, leaving the Department ill-prepared to defend against the escalating cyber threats of today and tomorrow.

This failure is not just an administrative oversight; it is a breach of the Department's legal and ethical obligations to protect the United States from cyber threats. The continued inability to comply with EO 13800 reflects a pattern of systemic negligence that transcends administrations and leadership changes. If these deficiencies are not addressed immediately and comprehensively, the consequences could be catastrophic, compromising national security, undermining public trust, and eroding the nation's ability to defend itself in an increasingly hostile digital landscape.

The OSD IT Digital Modernization Roadmap FY2026-2030, crafted under the leadership of Secretary of Defense Lloyd Austin, reveals an alarming pattern of willful negligence regarding the Department's cybersecurity responsibilities. Extending through 2030, this roadmap not only spans the current administration but also stretches into the administration beginning in 2029, potentially binding the hands of two future administrations with a deeply flawed strategy. This timeline reflects a troubling intent to perpetuate systemic failures in cybersecurity compliance, ensuring that critical vulnerabilities remain unaddressed regardless of leadership changes.

By the time this roadmap was developed, Secretary Austin would not have known the results of the recent election, which saw Vice President Kamala Harris lose decisively to President Trump. Regardless of the election outcome, the roadmap's timeline suggests a deliberate attempt to extend non-compliance with EO 13800 and the NIST Cybersecurity Framework (NIST CSF) well into the future. This planning raises serious concerns about whether the current Secretary of Defense intended to entrench a course of action that would delay or even obstruct meaningful reforms under future leadership. By doing so, Austin has effectively deferred responsibility for addressing the Department's cybersecurity failures to successors, creating a situation where systemic vulnerabilities are likely to persist for years.

The roadmap's deficiencies are glaring. It fails to explicitly align its initiatives with the NIST CSF's five core functions: Identify, Protect, Detect, Respond, and Recover. Without this alignment, the Department lacks the comprehensive risk management framework necessary to secure critical infrastructure against escalating cyber threats. This oversight is not a minor administrative lapse—it is a breach of federal law and a direct violation of EO 13800's mandate to integrate these functions into all cybersecurity efforts. By neglecting these foundational principles, the roadmap ensures that vulnerabilities remain unaddressed, leaving critical systems exposed to adversaries.

The timeline also suggests an alarming lack of urgency in addressing these issues. Stretching to 2030, this roadmap effectively kicks the can down the road, delaying necessary reforms until they become the responsibility of future administrations. This approach not only undermines the ability of the incoming administration to enact

meaningful changes but also extends these failures into the next administration beginning in 2029. Such a strategy risks institutionalizing non-compliance as a permanent feature of the Department's operations, creating a legacy of neglect that future Secretaries of Defense will struggle to reverse.

The roadmap's failure to enforce compliance with federal standards like NIST SP 800-53, SP 800-171, SP 800-161, SP 800-30, and SP 800-37 is another critical oversight. These standards provide detailed frameworks for securing systems, managing supply chain risks, and ensuring resilience against cyber threats. Yet, the roadmap offers no actionable measures for achieving compliance. For example, while it emphasizes cloud adoption, it does not specify how data will be encrypted, how access will be managed, or how vendors will be held accountable for adhering to federal standards. Similarly, its focus on artificial intelligence (AI) integration fails to address the unique risks associated with adversarial manipulation and data poisoning. These omissions are not just technical deficiencies—they reflect a deliberate disregard for the protections required by law to secure the nation's defense infrastructure.

Even more troubling is the roadmap's lack of accountability mechanisms. EO 13800 mandates that agencies demonstrate measurable progress in improving cybersecurity resilience, yet the roadmap focuses on operational milestones like cloud migration and DevSecOps adoption rather than outcomes like reduced vulnerabilities or faster incident response times. This deliberate avoidance of quantifiable metrics shields leadership from scrutiny and ensures that the roadmap's ineffectiveness remains hidden. Without transparency and accountability, the Department's cybersecurity efforts are destined to fail, perpetuating a cycle of neglect that leaves the nation vulnerable to attack.

The implications of this roadmap are profound. By extending its flawed strategy into the late 2020s and early 2030s, Austin has ensured that systemic vulnerabilities will persist across two future administrations, regardless of political leadership. This timeline creates a dangerous continuity of non-compliance that undermines the nation's ability to defend itself against escalating cyber threats. Whether this was done out of negligence, incompetence, or deliberate intent, the result is the same: a Department of Defense that remains unprepared to face the challenges of modern cyber warfare.

This failure also represents a profound breach of the constitutional oath taken by the Secretary of Defense to protect the United States from all threats, foreign and domestic. Cybersecurity is not a peripheral concern—it is a core component of national defense. By failing to comply with EO 13800 and federal standards, Austin has violated this oath, placing the safety and security of the American people at risk.

His actions—or inactions—are a betrayal of the trust placed in the Department to defend the nation's interests, both in the physical and digital realms.

The OSD IT Digital Modernization Roadmap FY2026-2030 is not just a flawed strategy; it is a damning indictment of the Department's leadership under Secretary Lloyd Austin. Its refusal to prioritize compliance with EO 13800 and the NIST CSF is a deliberate choice to ignore the legal and ethical obligations that safeguard the nation's defense infrastructure. This roadmap binds future leadership to a course of action that perpetuates the systemic failures of the past, ensuring that vulnerabilities remain unaddressed and adversaries remain emboldened. Without immediate action to correct these deficiencies, the Department risks leaving the nation exposed to catastrophic cyberattacks that could compromise its security and sovereignty for years to come.

The OSD IT Digital Modernization Roadmap FY2026-2030 builds on previous strategies, presenting itself as a forward-looking vision for transforming the Department of Defense's IT infrastructure and operational capabilities. While this roadmap demonstrates some progress compared to earlier strategies, including the 2019 DoD Digital Modernization Strategy and the 2022 Software Modernization Strategy, it remains deeply flawed. The most glaring issue is its continued inability to meet the requirements of EO 13800 and the NIST Cybersecurity Framework (NIST CSF). Although there are incremental improvements in certain areas, the roadmap ultimately fails to close the systemic gaps that leave the DoD vulnerable to escalating cyber threats.

One notable area of progress is the roadmap's greater emphasis on operationalizing modernization initiatives. Unlike previous strategies, which were heavily aspirational, the FY2026-2030 roadmap includes a clearer focus on implementing DevSecOps practices and expanding cloud adoption. These steps indicate an increased awareness of the importance of integrating security into the development lifecycle and leveraging scalable technology to meet mission demands. However, this progress remains superficial without a strong foundation of compliance with federal cybersecurity mandates. The roadmap's failure to explicitly align its initiatives with the five core functions of the NIST CSF—Identify, Protect, Detect, Respond, and Recover—undermines its effectiveness. These functions are the backbone of any comprehensive cybersecurity strategy, yet the roadmap neglects to show how its goals serve to identify vulnerabilities, protect critical systems, detect threats, respond to incidents, or recover operations.

In terms of cloud security, the roadmap reflects a growing commitment to cloud-native architectures, emphasizing scalability, interoperability, and efficiency. This is a step forward compared to the earlier strategies, which often treated cloud adoption as a vague aspiration rather than an actionable objective. Yet, the roadmap fails to

address the significant cybersecurity challenges inherent in cloud environments. Federal standards like NIST SP 800-171 and SP 800-53 mandate encryption, access controls, and continuous monitoring for all cloud systems, but the roadmap provides no actionable plans for implementing these measures. Additionally, it continues to overlook the critical need for supply chain security, particularly in managing third-party cloud vendors. This gap is consistent with previous strategies and highlights an ongoing failure to address vulnerabilities in the broader ecosystem of vendors and partners on which the DoD relies.

The supply chain remains one of the most significant unresolved issues in the roadmap. Despite the escalating threat landscape and the lessons learned from high-profile supply chain attacks, the roadmap does not adequately incorporate the guidance provided by NIST SP 800-161 for managing supply chain risks. It lacks measures to evaluate vendor compliance with federal standards, conduct regular audits, or monitor third-party dependencies for vulnerabilities. Compared to the 2022 Software Modernization Strategy, this roadmap demonstrates no meaningful progress in this area. The continued absence of a structured approach to supply chain risk management leaves the Department exposed to adversaries who increasingly exploit these weaknesses to gain access to critical systems.

Another persistent gap is the absence of robust incident response and recovery plans. While the roadmap emphasizes resilience, it provides no actionable details on how the Department will prepare for or recover from cyber incidents. EO 13800 explicitly requires federal agencies to develop and test comprehensive incident response protocols, yet this roadmap offers little beyond broad statements of intent. The failure to prioritize the Respond and Recover functions of the NIST CSF mirrors the shortcomings of earlier strategies. Without detailed response procedures, regular testing through red-teaming exercises, and secure off-site backups, the DoD remains unprepared to mitigate the damage from inevitable cyberattacks.

Metrics and accountability are areas where some improvement is visible. The roadmap introduces more operational milestones than its predecessors, with clearer goals for expanding DevSecOps pipelines and integrating AI capabilities. However, it still falls short of establishing meaningful cybersecurity metrics, such as vulnerability reduction rates, incident detection times, or compliance with NIST standards. EO 13800 requires demonstrable progress in enhancing cybersecurity resilience, and the roadmap’s continued focus on operational outputs rather than measurable outcomes reflects a failure to meet this mandate. This lack of accountability undermines the roadmap’s credibility and obscures the true state of the Department’s cybersecurity posture.

Legacy systems, often described as the Achilles’ heel of the DoD’s IT infrastructure, remain a critical vulnerability. The roadmap, like its predecessors, fails to present a

clear plan for assessing, securing, or replacing these outdated systems. Comprehensive risk assessments, interim protections, and phased migration plans are essential for managing these systems in accordance with NIST SP 800-30 and SP 800-37. Without addressing the vulnerabilities posed by legacy systems, the roadmap leaves critical gaps in the Department's defenses, perpetuating risks that adversaries are well-positioned to exploit.

Workforce development is another area that has seen incremental progress. The roadmap recognizes the importance of equipping personnel with the skills needed to implement and manage modernization initiatives. Compared to earlier strategies, there is greater emphasis on training and certification. However, this progress is undermined by the lack of a comprehensive strategy for recruiting and retaining top cybersecurity talent. Certifications in DevSecOps, cloud security, and AI risk management should be mandatory for relevant roles, and competitive compensation must be offered to attract and retain skilled professionals. Without investing in its workforce, the Department will continue to struggle with implementing its roadmap effectively.

Looking ahead, the roadmap must undergo significant changes to achieve compliance with EO 13800 and the NIST CSF. These changes must include a detailed mapping of all initiatives to the NIST CSF's five core functions, ensuring that every goal contributes to identifying vulnerabilities, protecting systems, detecting threats, responding to incidents, and recovering operations. Cloud security must be prioritized, with enforceable controls for encryption, access management, and continuous monitoring. Supply chain risk management must be integrated into every aspect of the roadmap, ensuring that third-party vendors are held accountable for meeting federal standards.

The Department must also develop and test comprehensive incident response and recovery plans, providing detailed procedures for mitigating damage and restoring operations after a breach. Metrics and accountability must be enhanced, with quantifiable measures for evaluating progress and regular audits to ensure transparency. Legacy systems must be addressed through phased modernization efforts, supported by robust interim protections. Finally, workforce development must be expanded to ensure that the Department has the expertise needed to execute its modernization goals effectively.

While the OSD IT Digital Modernization Roadmap FY2026-2030 demonstrates some progress compared to earlier strategies, its continued failure to address critical cybersecurity gaps represents a breach of the Department's legal and ethical obligations. The roadmap's inability to comply with EO 13800 and federal standards is not just a failure of execution—it is a failure of leadership. Without immediate and decisive action to correct these deficiencies, the Department risks perpetuating the

same vulnerabilities that have undermined its security posture for years, leaving the nation exposed to the escalating threats of the digital age.

OSD IT Digital Modernization Roadmap FY2026-FY2030.pdf
https://docdro.id/GBSIpQ8%0A

The cybersecurity strategies crafted by the Department of Defense—whether the 2019 Digital Modernization Strategy, the 2022 Software Modernization Strategy, the 2023 Software Modernization Implementation Plan, or the 2023 DoD Cyber Strategy Summary—are ostensibly aimed at protecting the systems, networks, and data critical to national defense. However, these documents often fall short in defining with precision what the DoD is meant to defend, leaving significant gaps in clarity, prioritization, and execution. Without a clear articulation of what is being safeguarded and why, these strategies risk failing to align their objectives with the realities of modern warfare, where cyber threats can destabilize both military and civilian infrastructure. To fully understand these shortcomings, one must examine what the DoD is tasked with defending and how well these strategies address—or fail to address—those responsibilities.

At its core, the DoD's mission is to defend the United States against all threats, foreign and domestic. In the digital era, this includes protecting the systems that underpin national defense, ensuring mission readiness, and maintaining the ability to deter and respond to adversarial actions in cyberspace. While these goals are often broadly referenced in the strategies, the specifics of what must be defended remain frustratingly vague. For instance, the DoD oversees some of the most sensitive and interconnected networks in the world, from command-and-control systems coordinating military operations to logistics networks ensuring the flow of supplies and reinforcements. These are not abstract concepts; they are tangible, critical assets that adversaries are actively targeting to degrade the United States' defense capabilities.

One of the most glaring issues in these strategies is their failure to prioritize which assets and systems are the most critical. Not all systems are created equal, and not all vulnerabilities carry the same risk. For example, a vulnerability in a weapons platform or a communications network used for battlefield coordination would have far graver consequences than a breach in a non-operational administrative system. Yet, these strategies rarely differentiate between systems of varying importance. This lack of prioritization dilutes the focus of cybersecurity efforts, spreading resources too thin and leaving the most vital assets insufficiently protected.

Furthermore, the strategies touch on the defense of classified and sensitive data, but the depth of this discussion is often inadequate. The DoD holds troves of intelligence, military plans, and research data that adversaries would consider high-value targets. A

breach of this information could compromise national security, reveal vulnerabilities in weapons systems, or even endanger lives. Despite the critical nature of this data, the strategies often fail to detail how it will be safeguarded comprehensively. Encryption, access controls, and real-time monitoring are mentioned in passing but are not given the granular attention they deserve. Without concrete measures tied to these goals, the DoD risks undermining its ability to protect one of its most valuable assets: information.

The role of the DoD in defending critical infrastructure is also inadequately addressed. While these strategies acknowledge that military operations rely on infrastructure like energy grids, transportation networks, and communication systems, they often stop short of defining the Department's role in defending civilian assets that are essential to mission readiness. For instance, a cyberattack on a civilian power grid could cripple the ability of military bases to operate effectively. Similarly, disruptions to supply chains—many of which rely on private-sector logistics networks—could hinder the deployment of troops and supplies. Despite these clear interdependencies, the strategies lack a robust discussion of how the DoD collaborates with other agencies, such as the Department of Homeland Security, to secure civilian critical infrastructure. This omission creates a dangerous blind spot in national cybersecurity planning, as the line between military and civilian infrastructure continues to blur.

Another critical component missing from these strategies is a clear articulation of how the DoD protects its global partnerships. The United States does not operate in isolation; its military and cybersecurity efforts are deeply intertwined with those of allies and international partners. These relationships are invaluable for intelligence sharing, joint operations, and collective defense against adversaries. However, partnerships also introduce risks, as weaker cybersecurity practices in allied networks can create entry points for adversaries to exploit. While these strategies emphasize the importance of collaboration, they fail to detail how the DoD ensures that partners adhere to rigorous cybersecurity standards. Without a framework for managing these risks, the DoD's global network remains vulnerable to exploitation.

The strategies also fail to address the growing challenge of defending against cyberattacks targeting the private sector. While not traditionally within the DoD's purview, private-sector companies play a critical role in national defense, particularly in areas like weapons manufacturing, satellite communications, and logistics. Cyberattacks on these companies could have cascading effects on military operations, yet the DoD's strategies largely ignore this dimension of cybersecurity. A more integrated approach, where the DoD collaborates with private-sector partners to enhance their cybersecurity resilience, is sorely needed but conspicuously absent.

Finally, the strategies often neglect to define the DoD's role in defending against emerging threats in cyberspace, such as ransomware, supply chain attacks, and AI-driven cyberattacks. These tactics are becoming increasingly common and sophisticated, yet the strategies rarely discuss how the Department plans to adapt its defenses to address them. For example, ransomware attacks could lock the DoD out of critical systems during a time-sensitive operation, while supply chain attacks could compromise the integrity of hardware and software used in military networks. The absence of detailed plans to counter these specific threats reflects a troubling lack of foresight and adaptability.

In summary, the DoD's cybersecurity strategies fail to adequately define what exactly they are defending and how they plan to achieve those objectives. While broad goals like defending critical infrastructure, safeguarding data, and ensuring mission readiness are mentioned, these strategies lack the specificity, prioritization, and accountability needed to translate those goals into actionable outcomes. To fulfill its mission, the DoD must develop a comprehensive and detailed understanding of what must be defended, prioritizing the most critical assets and systems while accounting for the interdependencies between military, civilian, and private-sector infrastructure. Without this clarity, these strategies will continue to fall short, leaving the United States vulnerable to the escalating cyber threats of the modern era.

The Iranian-backed cyberattack targeting Kash Patel, a former Trump administration official and the nominee for FBI Director under President Trump's incoming administration, exposes a grave vulnerability in the cybersecurity frameworks ostensibly designed to protect high-value targets in the U.S. government. This incident underscores a broader failure of the Department of Defense and other federal agencies to fully implement the protections mandated by EO 13800 and the NIST Cybersecurity Framework (NIST CSF)—protections intended not just to safeguard infrastructure but to shield individuals who are critical to national security. The attack reveals systemic gaps in how the nation approaches cybersecurity for key personnel, particularly those who possess or have had access to classified information.

Kash Patel, as a former official with a significant security clearance and an anticipated leadership role in one of the country's top intelligence agencies, represents exactly the kind of high-value target adversaries like Iran seek to exploit. The fact that Iranian hackers were able to target him so effectively demonstrates the inadequacy of existing measures to monitor, protect, and mitigate risks to such individuals. The incident raises immediate concerns about whether the Department of Defense, which played a pivotal role in cybersecurity policy development during Patel's tenure, has willfully neglected its obligations to protect even its former key personnel. This neglect reflects a broader institutional failure to comprehend and counter the cyber threat landscape of today.

The foundation of effective cybersecurity lies in robust risk management protocols, yet there is no evidence that Patel was under any enhanced protective measures despite his known prominence and sensitive past roles. NIST SP 800-37, the Risk Management Framework, explicitly calls for identifying high-risk individuals and assets, ensuring that appropriate safeguards are in place. In this case, the absence of such safeguards allowed Iranian hackers to exploit vulnerabilities and access communications tied to Patel. The targeting of such an individual, widely known to be working on behalf of the United States' national security interests, should have been anticipated and preempted.

Equally troubling is the evident lack of incident response and recovery measures, as outlined in NIST SP 800-61. The attack was identified after the breach had already occurred, suggesting a reactive rather than proactive posture. If effective detection and mitigation systems were in place, such as continuous monitoring tied to advanced analytics, the attack could have been detected at its earliest stages and contained before critical data was compromised. The inability to prevent or swiftly respond to this breach not only undermines the confidence in national security systems but also emboldens adversaries who perceive these lapses as exploitable weaknesses.

The attack also highlights glaring deficiencies in personnel security, which is emphasized in NIST SP 800-53. Individuals like Patel, who hold or have held security clearances, represent unique cybersecurity challenges. They possess intimate knowledge of U.S. operations, strategies, and vulnerabilities, making them prime targets for adversaries. Their protection must extend beyond their tenure in office, particularly when their expertise remains pivotal to national security. In Patel's case, the lack of safeguards to protect his communications or mitigate exposure to cyber threats reflects an institutional failure to prioritize personnel security.

What makes this case particularly egregious is that it occurs in the broader context of a decade-long failure to comply with federal cybersecurity mandates. EO 13800, signed into law to ensure that federal agencies adhere to the NIST CSF, laid out clear requirements for managing cybersecurity risks comprehensively. Yet, the Department of Defense and related agencies have consistently fallen short of meeting these standards, even after repeated breaches and public scrutiny. The systemic non-compliance suggests a pattern of negligence so persistent that it begins to resemble intent. The repeated failure to protect critical assets—whether systems, infrastructure, or personnel—raises legitimate concerns about whether this negligence is deliberate, creating a vulnerability that adversaries like Iran are eager to exploit.

The implications of this breach are profound. By failing to protect individuals like Patel, the DoD is not only exposing those with critical national security knowledge to harm but also jeopardizing the integrity of the systems they once helped manage. Patel's targeted attack serves as a stark reminder that cybersecurity cannot be

confined to networks and databases; it must encompass the people who make up the fabric of national defense. Adversaries recognize the value of targeting such individuals, and the U.S.'s inability to anticipate and counter these attacks reflects a lack of strategic foresight that is both reckless and dangerous.

This incident underscores the DoD's broader breach of its constitutional obligations to protect the United States against foreign threats. It highlights how the Department's repeated failure to comply with EO 13800 and align with the NIST CSF constitutes a direct violation of federal law and national security protocols. These frameworks were established not as bureaucratic exercises but as critical tools to safeguard the nation from exactly this kind of threat. By ignoring them, the DoD has left key figures like Patel exposed, undermining both their safety and the security of the nation as a whole.

The Iranian-backed attack on Patel is not an isolated incident but a symptom of a systemic failure. It reflects an institutional culture that has deprioritized compliance with cybersecurity mandates, failed to adapt to evolving threats, and neglected the protection of individuals who are integral to national security. Without immediate action to address these failures, the United States will remain vulnerable to adversaries who exploit these gaps with increasing frequency and sophistication. This case serves as a wake-up call for the DoD to finally prioritize compliance, accountability, and the protection of all assets—both digital and human—that contribute to the defense of the nation.

The Salt Typhoon hack, one of the most devastating cyberattacks on U.S. telecommunications infrastructure in history, lays bare the catastrophic failure of the Department of Defense to meet its cybersecurity obligations. Coupled with the SolarWinds hack in 2020, these attacks expose a relentless pattern of negligence stretching across successive Secretaries of Defense—Marc Esper under President Trump and Lloyd Austin under President Biden. These men, entrusted with safeguarding the nation's defense infrastructure, presided over strategies that were either grossly inadequate or willfully designed to delay meaningful action. Their failures reflect a systemic inability to adhere to EO 13800, a legally binding mandate to align federal cybersecurity defenses with the NIST Cybersecurity Framework (NIST CSF).

Salt Typhoon's timing, coming just weeks after a presidential election and echoing the SolarWinds breach four years prior, highlights a glaring vulnerability: adversaries know exactly when the U.S. is weakest. These are not random attacks; they are calculated moves to exploit moments of transition, uncertainty, and disorganization within the federal government. Yet despite the obvious patterns, the Department of Defense has done little—if anything—to close these vulnerabilities. In fact, the strategies under Esper and Austin have perpetuated this negligence, allowing

adversaries like China and Russia to repeatedly infiltrate critical systems, including those tied to national security and infrastructure.

Marc Esper's tenure as Secretary of Defense was marked by the rollout of the 2019 Digital Modernization Strategy, which should have served as a foundation for securing DoD systems and aligning with EO 13800. Instead, it was a vague, aspirational document devoid of actionable measures to combat real-world threats. The SolarWinds hack, which occurred near the end of Esper's tenure, infiltrated federal agencies and defense systems, compromising sensitive data and exposing glaring weaknesses in supply chain security. This breach, like the theft of Navy submarine data by Chinese hackers in 2018, was a direct result of systemic non-compliance with federal cybersecurity standards. NIST SP 800-161, which mandates rigorous supply chain risk management, was ignored, leaving contractors and vendors as open doors for adversaries. Esper had both the legal obligation and the resources to act but failed to implement even the most basic safeguards required by EO 13800.

Esper's inaction, however, pales in comparison to the failures of his successor, Lloyd Austin. While Austin inherited the DoD's systemic issues, he had the benefit of hindsight. The lessons of SolarWinds, CrowdStrike, and other breaches were well-documented by the time he assumed office. Yet under his leadership, the Department doubled down on vague strategies and long-term roadmaps that did little to address immediate vulnerabilities. The 2023 Cyber Strategy Summary and the OSD IT Digital Modernization Roadmap FY2026-2030 exemplify this approach, offering broad commitments without actionable steps to secure systems, protect personnel, or adapt to a rapidly evolving threat landscape.

Austin's decision to extend the roadmap to 2030 is not just ill-conceived—it is reckless. Cybersecurity is a field that changes by the day, let alone by the decade. Planning so far into the future without adaptive mechanisms is an abdication of responsibility. By the time these strategies are fully implemented, they will be outdated relics, incapable of addressing the threats of 2030. Worse, this extended timeline ensures that the failures of the DoD's cybersecurity posture will persist well into the next administration and beyond. It is a roadmap not to modernization but to continued vulnerability, designed to delay accountability and avoid the hard decisions necessary to secure the nation.

The timing of these attacks raises further questions about intent and responsibility. The SolarWinds hack in 2020 and the Salt Typhoon attack in 2024 both occurred during presidential transitions, moments when federal systems are stretched thin and the nation is most exposed. Adversaries have clearly identified these periods as opportunities to strike, yet the DoD has failed to adapt its strategies to anticipate and counter these predictable threats. This failure is not just negligence—it is willful blindness to the realities of modern cyber warfare. The persistence of these attacks

suggests that adversaries view the U.S. as a soft target, emboldened by the DoD's repeated inability to defend its systems and personnel.

Salt Typhoon's targeting of telecommunications infrastructure is particularly damning. The telecom sector, classified as critical infrastructure under EO 13800, is a cornerstone of both civilian life and military operations. The theft of metadata, including communications involving government officials, demonstrates a failure to implement even basic protections for one of the nation's most sensitive sectors. This breach mirrors the failures seen in SolarWinds and the earlier theft of Navy submarine data, underscoring a pattern of systemic disregard for supply chain security, real-time threat detection, and incident response.

These failures are not merely technical oversights but breaches of the constitutional duty to protect the United States from all threats, foreign and domestic. EO 13800 and the NIST CSF provide clear, enforceable standards to secure critical systems, yet the DoD under both Esper and Austin has chosen to ignore them. This negligence, spanning two administrations and two Secretaries of Defense, is not just incompetence—it is a betrayal of the American people. When viewed in the context of repeated breaches and escalating threats, this pattern of inaction begins to look less like failure and more like intent. The refusal to act in the face of clear and present dangers is tantamount to complicity, allowing adversaries to exploit weaknesses that should have been addressed years ago.

The consequences of this negligence are profound. The repeated breaches of federal systems, critical infrastructure, and private-sector partners have eroded public trust and weakened the nation's defensive posture. Each attack emboldens adversaries, who see the DoD's inaction as tacit permission to continue their operations. The damage is not just operational but strategic, undermining the credibility of the United States as a global leader in cybersecurity and defense. The failures of Marc Esper and Lloyd Austin have left the nation exposed, not only to external threats but also to the internal rot of a system that refuses to hold itself accountable.

The roadmap to 2030 is a glaring example of this refusal. In a world where cyber threats evolve daily, the idea of a decade-long strategy is not just naive—it is dangerous. These strategies will not protect the nation; they will ensure its continued vulnerability. The DoD does not need roadmaps to the future; it needs immediate, decisive action to address the failures of the past and secure the systems of the present.

Salt Typhoon is not just a wake-up call—it is a damning indictment of the DoD's systemic failures under Marc Esper and Lloyd Austin. Their negligence has left the United States exposed to repeated attacks, undermining national security and violating the constitutional oath to protect the nation. This cannot be allowed to

continue. The time for vague commitments and long-term roadmaps is over. The DoD must act now, not just to repair the damage already done but to restore the trust and security it has so recklessly squandered.

The SolarWinds and Salt Typhoon cyberattacks stand as stark illustrations of the evolving sophistication in adversarial tactics and the profound consequences of the Department of Defense's failure to implement robust cybersecurity protocols, such as those outlined in the NIST Cybersecurity Framework (CSF). These incidents are not isolated but part of a consistent pattern where attackers have exploited systemic vulnerabilities that adherence to the NIST CSF could have mitigated or even prevented. By examining the technical specifics of these attacks in detail, it becomes evident how critical functions within the CSF—Identify, Protect, Detect, Respond, and Recover—remain inadequately addressed, leaving the U.S. exposed to repeated cyber intrusions.

In the SolarWinds attack of 2020, adversaries leveraged a sophisticated supply chain compromise to infiltrate multiple federal and private networks. The attackers gained access to SolarWinds' software development environment, embedding malicious code into legitimate updates for the Orion software platform. This trojanized update, once deployed by unsuspecting customers, established a backdoor, dubbed SUNBURST, that enabled attackers to monitor and manipulate systems undetected. The success of this breach lay in the meticulous planning and advanced operational security demonstrated by the attackers. They employed domain generation algorithms (DGA) to obfuscate command-and-control (C2) communication and dynamically redirect network traffic to evade detection.

Had the NIST CSF been rigorously applied, several aspects of this attack could have been mitigated. Under the Identify function, a comprehensive understanding of dependencies on third-party software would have prompted stricter vendor security evaluations. Additionally, a robust risk assessment, as mandated by NIST SP 800-30, would have flagged the software development environment as a high-value target, necessitating additional protections. The Protect function, emphasizing secure software development practices and continuous code integrity checks, could have detected tampering before malicious updates were distributed. Furthermore, continuous monitoring as part of the Detect function could have identified anomalies in network traffic caused by the SUNBURST backdoor.

The Salt Typhoon attack, revealed in 2024, further underscores the systemic failures in cybersecurity preparedness. This Chinese state-sponsored group targeted U.S. telecommunications networks, exploiting vulnerabilities in network infrastructure components such as routers, switches, and firewalls. The attackers utilized a combination of living-off-the-land (LOTL) techniques and highly customized malware to maintain persistence and evade detection. By using legitimate

administrative tools already present in the compromised environment, they blended their activities with normal operations, making traditional signature-based detection methods ineffective.

Salt Typhoon's success highlights critical gaps in the Protect and Detect functions of the NIST CSF. For instance, timely application of security patches, a basic tenet of the Protect function, could have mitigated vulnerabilities in network devices that the attackers exploited. The Detect function emphasizes the use of advanced threat detection systems capable of identifying behavior anomalies rather than relying solely on known signatures. Machine learning-based intrusion detection systems, as recommended in NIST SP 800-53, could have flagged the irregularities introduced by LOTL techniques.

The timing of these attacks during presidential transitions is particularly damning. The SolarWinds breach coincided with the 2020 election transition, while Salt Typhoon unfolded during the 2024 transition. These moments of upheaval and resource reallocation present predictable vulnerabilities that adversaries have exploited repeatedly. The Respond and Recover functions of the NIST CSF, which focus on swift containment and restoration of systems during and after a breach, were glaringly absent. Incident response plans, which should include scenarios for supply chain attacks and infrastructure intrusions, were either underdeveloped or entirely lacking. Regular red-teaming exercises, as recommended by NIST SP 800-84, could have exposed these blind spots and better prepared agencies for such predictable adversarial behavior.

The CrowdStrike breaches, the 2018 theft of Navy submarine data, and other documented hacks further illustrate the long-standing systemic issues. Adversaries have consistently exploited weak vendor security protocols, inadequate monitoring, and an overreliance on traditional defenses like firewalls and antivirus solutions. For example, the theft of Navy submarine data was facilitated by weak access controls and poor segmentation of classified and unclassified networks—failures directly addressed by NIST SP 800-171, which mandates stringent controls for protecting controlled unclassified information (CUI). Yet, despite these clear mandates, systemic non-compliance continues, leaving critical systems vulnerable to compromise.

The broader implications of these failures are staggering. The DoD's persistent inability to align with the NIST CSF not only violates federal law under EO 13800 but also perpetuates a cycle of vulnerability that adversaries exploit with increasing regularity. The roadmap to 2030, introduced under Secretary of Defense Lloyd Austin, is emblematic of this failure to act decisively. By proposing strategies that lack specificity and urgency, and by stretching timelines well into the future, the DoD has effectively deferred accountability while leaving the nation exposed to present and future threats.

Moreover, the technical sophistication of these attacks—such as the use of domain generation algorithms, LOTL techniques, and customized malware—underscores the inadequacy of static, outdated defenses. Adherence to the NIST CSF demands dynamic, real-time adaptations to emerging threats, yet the DoD's strategies remain rooted in an outdated paradigm of defense. This failure to evolve alongside adversarial tactics is perhaps the most damning indictment of the Department's cybersecurity posture.

In conclusion, the technical intricacies of the SolarWinds and Salt Typhoon attacks, along with numerous other breaches, reveal systemic gaps in the DoD's implementation of the NIST CSF. These frameworks were designed to address precisely these kinds of threats, yet their incomplete or non-existent application has left the nation vulnerable. The repeated failures under Marc Esper and Lloyd Austin are not just lapses in judgment but betrayals of the constitutional duty to protect the nation. The sophistication of the adversaries should have been met with equal sophistication in defense. Instead, the Department's inaction has allowed these breaches to persist, eroding public trust and jeopardizing national security on an unprecedented scale.