Thank you for this opportunity to share a position paper on efforts to enhance the security of the software supply chain and to fulfill the President's Executive Order (EO) on Improving the Cybersecurity of the Federal Government, issued on May 12, 2021. EO 14,028 does well to call attention to the need to implement a modern cybersecurity approach within the United States Government. SailPoint welcomes the opportunity to contribute to the enhancement of the security of the nation's software supply chain.

Founded in 2005, SailPoint is an Austin, Texas-based technology company that is the leader in identity security for the cloud enterprise. The identity security solutions we provide both secure and enable thousands of companies worldwide, giving our customers unmatched visibility into the entirety of their digital workforce, and helping ensure that workers have the right access to do their job.

We see particular importance in Section 4 of the EO as delineated by NIST's recent call for position papers on standards and guidelines to enhance software supply chain security. SailPoint's response and position statements are focused on the third area as outlined in the call for papers: *Guidelines outlining security measures that shall be applied to the federal government's use of critical software,* including but not limited to, least privilege, network segmentation, and proper configuration. EO Section 4(I).

Least privilege and zero trust are currently *en vogue*, with good reason: the recent changes to social order have accelerated the digitalization of the workforce. The network perimeter is no longer a sufficient control in today's highly complex, ephemeral, and distributed application environment where software applications are developed and delivered in the cloud. Without the traditional network perimeter, security measures that appropriately protect critical software are dependent on identity, as reflected in the concept of "identity-defined security."

Certain identity-defined, zero trust security principles must be applied to the software supply chain including:

1) **Never trust, always verify:** Trust is explicit. Every user or agent accessing software must be authenticated and every transaction verified.
2) **Just enough, least privilege:** Users or agents should be given only the privileges necessary to complete a given task (no more, no less).
3) **Zero standing privileges or just in time:** Entitlements should be granted at the time of need and removed after use.
4) **Continuously monitor:** Activity and environmental risk factors must be continuously monitored, and mitigating controls applied; the efficacy of access controls must be continuously evaluated.

More specifically, SailPoint believes identity security and access governance technologies are essential components of a software supply chain security strategy. We believe that the NIST guidance should include recommendations for the items outlined in Table 1:

Identity lifecycle management	Identity is the cornerstone of identity defined security. All access decisions are based on an identity and the attributes associated with an identity record. The identity record must be maintained, and identity attributes continuously updated. User accounts in managed software applications should be provisioned, updated, and de-provisioned according to changes to the identity record and joiner, mover, leaver processes.
Least privilege access controls	Securing the software supply chain requires, as a basic measure, least privilege access controls for all software leveraged by 1st and

	3rd party entities. Least privilege access controls require the ability to apply complex policy logic, roles, policy-based access controls, and SOD controls. Ideally, least privilege access controls should be dynamic and auto-adjust based on changes in the environment. Broad sweeping, overprivileged group membership is the antithesis of least privilege.
Identity Correlation	The ability to correlate an entity (human or non-human) to an identity and associate that particular identity to user accounts, entitlements, and activity in software applications is critical. Identity correlation ensures that as issues arise, responsible parties can be identified.
Access Governance/Audit	Access governance provides answers to the proverbial question, "who has access to what?" The identity system should include an identity data warehouse that provides a 360 degree view of an identity and its related access. The warehouse should establish relationships between identities, user accounts, entitlements, and devices. The identity system must audit access across all facets of the software supply chain and determine if access is appropriate. Access governance not only provides an index of identities and entitlements, but also provides an evaluation of the effectiveness of access controls in the software supply chain environment.
Identity Automation and Access Intelligence	The ability to manage and govern access in a complex software environment has moved beyond human capacity. Next generation identity security systems should incorporate AI/ML and analytic technologies that adapt to changes in the environment and automatically detect and respond to threats in the environment.

SailPoint has global expertise in implementing identity-defined security and looks forward to the opportunity to help secure the software supply chain. However, we do not assume that the aforementioned functions live in isolation. We believe that a sound software supply chain security strategy should also include strong authentication, privileged access management, data access governance, software-defined network controls, software bills of materials (SBOM), and other security mechanisms.

SailPoint is encouraged by the EO and the Administration's focus on cyber security, and we appreciate the opportunity to respond to this call for position statements. We believe that identity security is the foundation of an effective supply chain security strategy. While the format of this response restricts the depth of our response, we look forward to participating in NIST's virtual workshop next week as well as having more detailed discussions with you. Specifically, we would be pleased to participate as a speaker at the workshop, and if permitted to participate would propose Grady Summers, Executive Vice President, Product, whose email address is grady.summers@sailpoint.com. We believe Mr. Summers can provide practical industry and technical insight that would be valuable to the workshop's objectives. Thank you again for this opportunity.