TECHNET
THE VOICE OF AMERICAN INNOVATION

1420 New York Avenue NW, Suite 825
Washington, D.C. 20005
www.technet.org | @TechNetUpdate

November 10, 2026

The Honorable Jay Clayton
Director of National Intelligence
Chair
White House Super Intelligence Force

The Honorable Andrew Ferguson
Chairman, Federal Trade Commission
Co-Chair
White House Super Intelligence Force

The Honorable Scott Kupor
Director, Office of Personnel Management
Co-Chair
White House Super Intelligence Force

The Honorable Emil Michael
Under Secretary of Defense for Research and Engineering
Co-Chair
White House Super Intelligence Force

Dear Chair Clayton and Co-Chairs Ferguson, Kupor, and Michael:

TechNet, the national, bipartisan network of technology CEOs and senior executives, appreciates the Trump Administration's commitment to ensuring that the United States remains the global leader in super intelligence (SI) while addressing the risks associated with its development and deployment. We welcome the establishment of the White House Super Intelligence Force (SI Force) and the opportunity to provide recommendations as it develops its report and plan for coordinating the federal government's approach to SI governance.

SI presents extraordinary opportunities to deliver meaningful benefits to all Americans. To provide these opportunities, the government and industry should take a practical approach that promotes public safety and addresses legitimate concerns regarding safety, security, accountability, and public trust.

We appreciate the SI Force's focus on key priorities, including cybersecurity, biosecurity, model accountability, implementation of the White House Accord, and federal incident reporting. As the SI Force advances this work, TechNet offers the following recommendations.

Leverage and Strengthen Federal SI Safety and Security Standards

The SI Force should build on the administration's existing efforts to advance technically grounded, measurable, and voluntary consensus-based safety and security standards. Rather than develop its own standards, the SI Force should leverage the work of the National Institute of Standards and Technology (NIST) and its Center for Advancing Innovation and Standards for Super Intelligence (CAISSI) to inform its recommendations, strengthen federal coordination, and avoid duplicative requirements.

NIST-led efforts should prioritize emerging risks from advanced and autonomous SI systems, including cyber threats, critical infrastructure vulnerabilities, and agents operating beyond their intended permissions. Relevant guidance should address secure development and testing, access controls, monitoring, and defense-in-depth safeguards that favor graduated controls over disruptive shutdown mechanisms. NIST and CAISSI should also advance open, interoperable standards for verifiable agent identity, exploring existing domain name and digital certificate infrastructure to strengthen authentication, accountability, and incident reporting. The SI Force's recommendations should preserve risk-based flexibility, avoid extending frontier-specific expectations to lower-risk AI systems, and ensure voluntary technical standards are not converted into mandatory regulatory requirements.

Support an Evidence-Based Assessment of Emerging SI Risks

TechNet welcomes the SI Force's decision to commission an assessment by the President's Council of Advisers on Science and Technology (PCAST) focused on cybersecurity and critical infrastructure protection, biosecurity and dual-use applications, and model control and accountability. The assessment should distinguish between demonstrated risks, emerging threats, and hypothetical scenarios while evaluating the likelihood, severity, and potential consequences of identified harms.

The assessment should also consider how risks vary across different SI capabilities, applications, and deployment environments. In particular, it should distinguish between risks arising from the development of advanced SI models and those associated with their integration into downstream applications or misuse by malicious actors. This distinction is essential to ensuring that safeguards are appropriately targeted and responsibilities are assigned to the entities best positioned to address them.

TechNet also encourages PCAST to evaluate the effectiveness of existing safeguards, industry practices, and federal authorities before recommending additional government intervention. Where gaps are identified, recommendations should be grounded in evidence and focus on concrete, actionable measures that can meaningfully reduce risks. The assessment should draw on expertise from industry, academia, standards organizations, and relevant federal agencies to ensure its findings reflect current technological capabilities and practical risk mitigation approaches.

Advance Practical SI Testing, Evaluation, and Safeguards

Effective SI governance requires practical testing methodologies, benchmarks, and evaluation frameworks to assess system performance, identify vulnerabilities, and verify that safeguards function as intended. As the SI Force develops its implementation plan for the White House Accord on Super Intelligence, it should establish clear expectations for how covered frontier AI developers assess and mitigate risks through capability testing, system monitoring, independent evaluations,

and vulnerability remediation, while preserving flexibility for internal research, development, and pre-deployment safety experimentation.

The SI Force should leverage existing federal investments in AI testing, evaluation, verification, and validation (TEVV), including NIST's AI Risk Management Framework and ongoing initiatives led by NIST and CAISSI in collaboration with industry. These efforts should support voluntary, reproducible evaluation methods and practical guidance for increasingly autonomous and agentic systems, including testing and reevaluation throughout the lifecycle. While the White House Accord focuses on frontier developers, broader voluntary NIST frameworks can support risk management across the AI ecosystem, with safeguards proportionate to the capabilities, uses, and risks of individual systems. The SI Force's recommendations should align with existing industry practices and internationally recognized frameworks, avoid duplicative or prescriptive requirements, and ensure that any broader regulatory proposals are grounded in demonstrated risks, existing legal authorities, and stakeholder engagement.

Establish a Clear and Coordinated Incident Reporting Framework

TechNet recognizes the importance of timely information sharing and coordinated responses to serious SI safety and security incidents. As the SI Force develops federal incident reporting mechanisms for frontier systems, it should establish clear, risk-based criteria that focus on confirmed incidents resulting in material, demonstrable harm to public safety, national security, or critical infrastructure. Reporting thresholds should distinguish between actual security incidents, credible threats, and routine testing results or expected system behaviors that do not present material risks. Crucially, pre-deployment evaluations and third-party benchmark testing must be explicitly protected from mandatory incident reporting so that aggressive safety testing is not disincentivized.

The framework should clearly define covered entities, reportable incidents, reporting timelines, responsible federal agencies, and expectations for remediation and follow-up, establishing clear role delineation across the AI value chain. Specifically, Cloud Service Providers (CSPs) and hosting infrastructure providers should not be obligated to monitor or report on customer-layer application incidents where they lack insight into customer data or operational control, placing reporting responsibilities appropriately on the deploying entity. Reporting obligations should be proportionate to the severity of an incident and the reporting entity's knowledge of and ability to address the underlying risks. Any mandatory reporting requirements should be appropriately scoped to the entities and risks they are intended to address and should not automatically extend frontier specific obligations to developers or deployers of lower-risk SI systems. The SI Force should also consider how to encourage early notification of serious incidents without creating incentives for overreporting, discouraging internal testing, or diverting resources from effective incident response.

Any new reporting mechanism should build on existing cybersecurity incident reporting and vulnerability disclosure frameworks such as CIRCIA, avoid duplicative

obligations, and provide robust statutory protections, including explicit exemptions from public records disclosures and liability safety harbors, for sensitive security information, proprietary data, and intellectual property. The SI Force should leverage existing federal guidance, including NIST, NSA, and CISA's work on incident readiness and response during advanced SI training and evaluation, rather than creating entirely new processes where established practices can be adapted.

The SI Force should also recognize the importance of coordinated vulnerability disclosure and provide companies with reasonable opportunities to investigate, contain, and remediate incidents. TechNet encourages the SI Force to engage industry in developing reporting protocols and to clearly identify the statutory authorities supporting any mandatory requirements. A consistent, proportionate approach will improve government visibility into serious risks while encouraging timely reporting, effective remediation, and continued collaboration between government and industry.

Develop an Actionable Implementation Plan Through Public-Private Collaboration

TechNet encourages the SI Force to set a clear agenda for the federal government implementation, including long-term and short-term priorities and specific actions that federal agencies should take using their existing authorities.

We recommend that the plan include:

- A government-wide inventory of existing SI-related legal authorities, regulatory requirements, standards, and guidance, including an assessment of duplication and potential gaps.

- A prioritized assessment of SI risks, drawing on PCAST’s findings and distinguishing between demonstrated threats, emerging risks, and areas requiring additional research.

- Specific recommendations for ensuring that federal actions are informed by and aligned with existing NIST efforts and advance NIST-led voluntary technical standards, TEVV methods and government TEVV capacity, and practical safeguards through NIST and other appropriate bodies.

- Clear agency responsibilities and coordination mechanisms to promote consistency in federal implementation and enforcement.

- Risk-based incident reporting protocols that align with existing cybersecurity frameworks including CIRCIA protections, limit reporting strictly to confirmed production harm, carve out pre-deployment red-teaming, and protect sensitive security and proprietary information.

- A process for regularly reviewing and updating federal guidance as SI capabilities, applications, and risks evolve, with meaningful opportunities for public and industry input.

Effective SI governance requires sustained engagement with a broad range of stakeholders, including frontier model developers, downstream innovators, open-source developers, small businesses, critical infrastructure operators, academia, and standards organizations. TechNet encourages the SI Force to establish a structured engagement process to ensure its recommendations are technically feasible, proportionate to identified risks, and informed by industry expertise. The implementation plan should also include measurable objectives to assess whether federal actions improve safety, security, and public trust without unnecessarily restricting innovation.

Conclusion

The SI Force presents an important opportunity to advance a coordinated federal approach to SI governance that protects Americans while supporting continued innovation. Its recommendations should build on existing authorities, leverage voluntary standards and safeguards, and provide clear, practical guidance while preserving flexibility to address evolving risks and capabilities.

TechNet and our member companies stand ready to work with the SI Force, PCAST, and relevant federal agencies to develop practical, evidence-based recommendations that strengthen public trust, protect consumers, and reinforce U.S. leadership in SI innovation.

Sincerely,



Linda Moore
President and CEO