Dr. Laurie E. Locascio,

Under Secretary of Standards & Technology,

National Institute of Standards and Technology (NIST).

Dr. Locascio,

We appreciate the opportunity to respond to the Request for Information (RFI) related to NIST's assignments under sections 4.1, 4.5 and 11 of Executive Order 14110.

We believe that NIST should focus on delivering an actionable security and safety solution that includes the following characteristics:

(1) deliver an **actionable** AI safety and security framework that builds on existing processes and procedures that are well-understood by both industry and agencies,

(2) map **NIST AI RMF** to existing NIST cybersecurity frameworks such as **800-53** and **CSF,**

(3) establish a **uniform** and **consistent** terminology around AI risk management and associated practices to allow industry to develop solutions based on standards.

Our comments are based on experience gathered in helping US Federal agencies transform their information technology systems and manage risk while adoption cloud computing a decade ago. In 2009, I assisted with the first migration of a government wide system to receive an ATO: Recovery.gov to Amazon Web Services (AWS). Since then, we have had the privilege of supporting numerous transformation initiatives as part of the GSA Centers of Excellence (COE) since 2018. We have contributed towards the development of the Cloud Adoption Playbook while supporting transformation engagements at USDA, HUD, NIH and OPM amongst others.

Our approach to AI Risk Management is rooted in using open standards and frameworks provided by NIST. We believe that NIST should enhance and adapt existing risk management practices as opposed to coming up with a brand-new approach to AI risk management. Mapping NIST AI RMF to NIST RMF, NIST SP 800-53 and governance models such as ATOs (Authority to Operate) through existing mechanisms such as Control Overlays for AI provide an accelerated implementation path to addressing AI specific risks like safety, bias and explainability.

Very respectfully, 02/01/2024

Gaurav Pal,

CEO & Founder

Our comments are centered on addressing the gaps in the Current standards or industry norms or practices for implementing AI RMF core functions for generative AI (govern, map, measure, manage), or gaps in those standards, norms, or practices.

Based on our interactions with industry, public sector leaders and experienced government and industry executives, the overwhelming consensus is to avoid creating a new governance model for AI. Instead, an approach that augments and enhances existing cybersecurity risk management frameworks to account for AI specific risks around safety, bias and explainability (SBE) can avoid costly delays in deploying safe AI systems in production. These views were also widely echoed by industry and government participants in the Meritalk Accelerate AI Forum held on Jan 30, 2024 at the City Club in Washington DC.

NIST should use its vast convening assets to develop an assessment and accreditation standard by mapping NIST AI RMF to **NIST SP 800-53** and **NIST CSF** using **Control Overlays** for **AI.**

AI Risk Management Accelerator: Map NIST AI RMF to NIST SP 800 & CSF

NIST AI RMF provides a great starting point to help define the initial corpus of threat and risk vectors from AI systems. However, there is a need for a prescriptive compendium that offers an implementable, assessable, and accreditable risk management model that is reasonably well understood and adopted by both industry, government, and public sector organizations.

Building upon existing cybersecurity risk management mechanisms focused on confidentiality, integrity and availability (CIA) and augmenting them with additional controls to address safety, bias and explainability (SBE) can deliver a complete solution. This approach is easily digestible and jumpstart CIO, CISO and Chief AI Officer (CAIO) to start thinking of accelerated ways to deploy AI systems.

NIST should take the following steps:

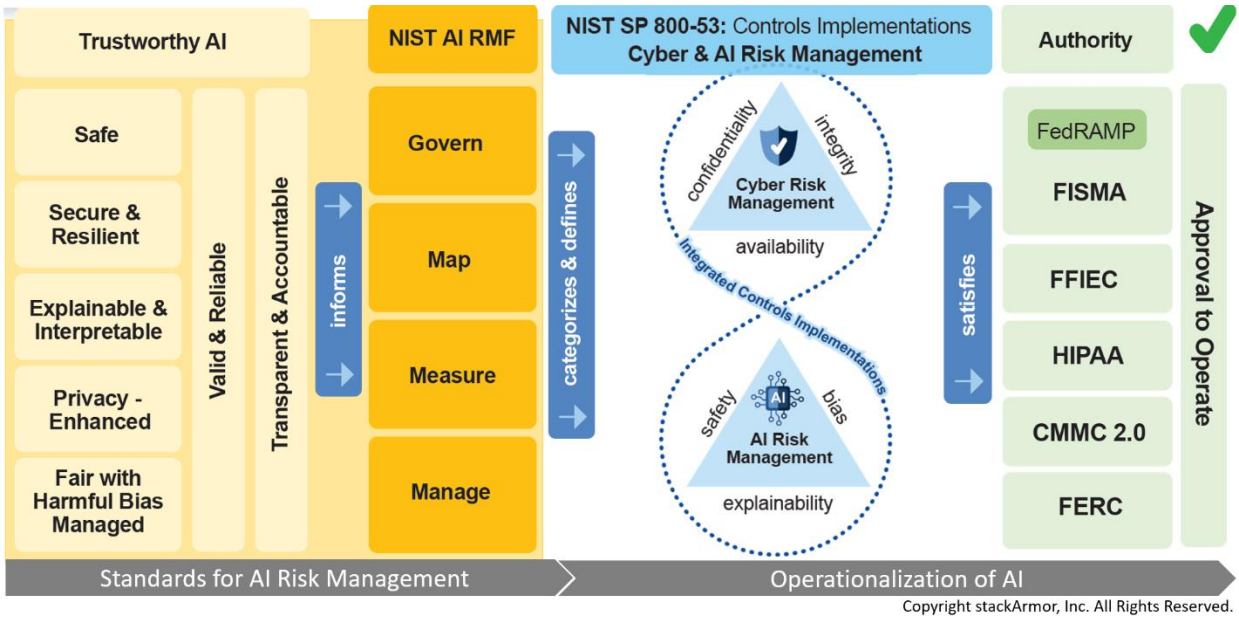
1) Map NIST AI RMF to existing cyber risk management models such as NIST RMF, NIST CSF, NIST SP 800-53 and NIST SP 800-53A as well as leverage the work done by the Federal Privacy Council, which provides an accelerated pathway to adopting secure and safe AI within the enterprise. The mapping should tailor existing controls for AI specific risks and provide new controls to address safety, bias, and explainability. The alternative pathway of creating a new governance model specifically for AI will be costly and delay the adoption of AI and lead to potential for Shadow AI especially in regulated entities.

2) Use of Control Overlays for AI to develop safety, bias and explainability related guardrails. We draw parallels with the evolution of the governance framework for cloud computing almost a decade ago. In 2010, Recovery.gov and Treasury.gov migrated to the commercial cloud and received an Authority to Operate (ATO). The governance model utilized NIST SP 800-53 Rev 3, that were augmented with cloud computing control overlays. Subsequently, the FedRAMP program was established, and cloud computing-aware controls were incorporated into SP 800-53 Rev 4. NIST can utilize its vast convening and collaboration

assets to bring together industry, academia, and government experts to deliver a first draft of the Control Overlay for AI that builds on NIST AI RMF.

3) ATO's are increasingly well understood by a rapidly growing segment of industry, government, public sector and state agencies. The FedRAMP program, StateRAMP and now CMMC 2.0 have established a broader understanding of a NIST based risk governance model. The security and compliance experts at stackArmor have developed a open and standards based governance model called ATO for AI™ that provides an initial mapping of NIST AI RMF risk categories to NIST SP 800-53 controls along with tailoring for AI specific risks.

Based on our experience helping agencies, commercial organizations and regulated entities implement security controls, we have developed an open and standards-based governance model that we call ATO for AI™. This model begins with the seven trustworthy characteristics of AI and the NIST AI RMF risk categories & sub-categories and maps them to the NIST SP 800-53 Rev 5 control families and controls. The model adds an AI Overlay construct that includes AI-specific controls not adequately covered by existing NIST SP 800-53 Rev 5 controls. The combination of tailored NIST SP 800-53 Rev 5 controls with Overlay Controls specific to AI provides an actionable and well-understood approach to risk management. The ATO for AI approach can accelerate the adoption of AI while reducing the time delays and costs of alternate approaches to AI risk management and governance. The infographic below provides an overview of our overall approach to AI risk management and governance.



Infographic demonstrating an end-to-end risk management and governance model that augments and builds upon existing processes, procedures and body of knowledge within an agency for AI

We have prepared detailed mappings of the controls and have vetted our approach by sharing it with the NIST public working groups on AI as well as leading industry and government executives as part of our AI Risk Management Centers of Excellence (CoE).

Members of our CoE include:

- Ms. Suzette Kent, former U.S. Federal CIO
- Ms. Maria Roat, former U.S. Deputy Federal CIO
- Mr. Richard Spires, former U.S. Department of Homeland Security CIO
- Mr. Alan Thomas, former commissioner of the GSA Federal Acquisition Service
- Ms. Teresa Carlson, transformational industry executive with over 25 years of leadership

Our COE members have rich operational and policy experience and have offered the following comments on our approach.

"Harnessing the power of AI for delivery of government mission and services will be transformational. But it is complicated to align all the emerging policy, risk frameworks, approval processes and existing policy and law. I am thrilled to be included in the COE because I have seen the work of the stackArmor team to drill down to details and find a path to connect all the pieces. We can only get to use of operational AI at scale by working through these details. I hope the output of the COE will deliver tools that agencies can use to move faster and to confidently scale AI capabilities."

Suzette Kent, Former Federal CIO. Ms. Kent as an extensive private and public sector background. As the Federal CIO, Ms. Kent was responsible for government-wide IT policies and spending, and also chaired the Federal CIO Council and the Technology Modernization Fund Board.

"The adoption of risk-based methods for managing and governing AI systems that leverage security controls defined in NIST SP 800-53 Rev 5 as well as established governance programs like FedRAMP can help agencies adopt AI more rapidly. Reducing the time and cost burden on agencies and supporting contractors by enhancing existing protocols is critical to ensuring timely deployment of AI systems for supporting the government mission."

Maria Roat, Former Deputy Federal CIO, SBA CIO and Director, FedRAMP PMO. Ms. Roat is a Senior Information Technology and Cybersecurity Executive with 3+ decades' experience driving enterprise-scale digital transformation within Federal Government. Recognized as builder, collaborator, and solutions innovator with vision, audacity, and drive to lead complex multibillion-dollar technology initiatives.

"Managing risk associated with AI systems is essential to ensuring Government's ability to improve agency effectiveness and efficiency using next generation AI and Automated Decision Support systems. stackArmor's systems engineering approach to applying NIST security controls to AI systems provides a reasonable blueprint for AI risk management."

Richard Spires, Former DHS, and IRS CIO. Mr. Spires provides advice to companies and government agencies in strategy, digital transformation, operations, and business development. He previously served as the Chief Information Office (CIO) of the U.S. Department of Homeland Security (DHS) and as CIO of the Internal Revenue Service (IRS).

"ATO for AI offers government agencies a fiscally prudent pathway to safe and secure AI adoption that builds upon lessons learned upon implementing existing governance frameworks like FISMA and FedRAMP. stackArmor's approach of operationalizing NIST AI RMF with actionable control implementations can help agencies accelerate safe AI systems adoption without having to retrain thousands of program, acquisition and IT specialists on new governance models for AI."

Alan Thomas, Former Commissioner, Federal Acquisition Service, GSA. Mr. Thomas is an Operating executive and former Federal political appointee with more than 25 years delivering mission critical programs, championing large scale digital transformation initiatives, and building deep functional expertise in acquisition and procurement.

"The unique combination of AI-enabled applications on cloud-computing powered services offers a once-in-a-generation opportunity to truly enable a digital-first government. Transforming legacy applications at scale by using accelerators that deliver safe and secure AI-native applications developed by innovative ISVs on FedRAMP accredited cloud service providers can help us dramatically shorten the time and cost of AI adoption."

Teresa Carlson, transformational industry executive with over 25 years of leadership in modernizing public sector organizations using commercial solutions including cloud computing.

We are prepared to offer our mappings of the NIST AI RMF to NIST SP 800-53 Rev 5 controls as well as the augmented overlays into the public domain to help accelerate NIST's efforts. You may download our whitepaper with additional information about our approach from our website https://www.stackArmor.com/AI