DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket Number: [210726-0151]

Artificial Intelligence Risk Management Framework

POC: Sally Kenyon Grant and John Abeles
Company Name: Lucd AI - d/b/a Deep Insight Solutions, Inc. and System 1, Inc.
Company Address: 424 Church Street, Suite 2000, Nashville, TN 37219 /
11810 Grand Park Avenue, #500, North Bethesda, MD 20852

I. Introduction for NIST AI RMF

System 1, Inc. and Lucd AI have formed a team (hereafter called the "Team") to respond to the National Institute of Standards and Technology (NIST) request for information for the development of a framework that can be used to improve the management of risks to individuals, organizations, and society associated with artificial intelligence (AI). The Team understands that the NIST Artificial Intelligence Risk Management Framework (AI RMF or Framework) is intended for voluntary use and to improve the ability to incorporate trustworthiness considerations into the design, development, and use, and evaluation of AI products, services, and systems. Our Team are both small businesses who are known for their innovation and the ability to formulate cost effective solutions.

Our Team has unique experience and understanding of the technical issues as well as societal issues relating to the genesis and maturity of AI and the inherent risks. System 1 has supported NIST in development the of various approaches and risk frameworks including the RMF and CSF (NIST 800 series documents, NISTIRs, special studies, training, and operational implementation). Our strength lies in managing and reducing risk cost effectively, cybersecurity, privacy, and critical infrastructure protection. Our Federal clients from the White House and Congress to the cabinet level agencies, over 20 of the National Laboratories, and the intelligence community. Our private sector clients include Fortune 100 companies in Energy, health sectors, and others. The tools we use are AI enabled so we understand some of the benefits and constraints during implementation. We have a history of brokering successful solutions across diverse communities that address a wide range of areas.

Lucd AI is leading the evolution of artificial intelligence. With the convergence of Big Data, Complex Distributed Systems, and the Internet-of-Things. The world is ready for true, strong AI that is able to extract knowledge and understanding from the world's largest repositories of structured and unstructured data. Lucd AI is delivering solutions derived from one of the world's most comprehensive developed intelligence platform. Lucd AI's innovative AI applications span global finance, energy, health, devices, social media and more. With the power of Lucd.AI, Lucd is solving not only today's most complex problems, but tomorrow's as well.

Lucd.AI combines human-like knowledge, understanding, and common-sense reasoning with the power, speed, and scalability of modern computing. More than three decades in development, and a generation ahead of any other AI solutions currently on the market, Lucd.AI is not just a competitive advantage; it's a disruptive technology that can transform industries, bring real clarity to seemingly intractable problems and ultimately help to make the world a better place. Lucd.AI accommodates new assertions and evidence with its existing theories and understanding of the world. Lucd. AI's reasoning engines contain inference modules that enable efficient, scalable inference, drawing conclusions from known facts, answering questions, and solving problems.

Lucd AI is currently working with the White House on an Agent-based Pandemic Modeling Framework to address the prediction and response of COVID-19 across the Combatant Commands.

In addition, Lucd.AI is the lead at the JAIC IL 4,5 with advanced cybersecurity protocols on all artificial intelligence and machine learning systems to include NIST 800-53 including approved and authorized by the Central Intelligence Agency (CIA) and National Security Agency (NSA). Lucd AI continues to dominate the world of data science with National Security measures by the usable and acceptable Single Sign-On Multi Factor Authentication (SSOMFA) utilizing the Central Authentication Service (CAS).

Most notably, Lucd.AI has built the most advanced cybersecurity artificial intelligence and machine learning systems in the U.S. Department of Defense for MAJCOMS providing a Technology Readiness Level-9 (TRL) mature of critical technology elements and a commercial off-the-shelf, turn-key-solution leveraging containerization, that is product customizable built and ready to be deployed in 45-days.

The Team's response to the RFI will address identify and better understand common challenges in the design, development, use, and evaluation of AI systems that might be addressed through a voluntary Framework; gain a greater awareness about the extent to which organizations are identifying, assessing, prioritizing, responding to, and communicating AI risk or have incorporated AI risk management standards, guidelines, and best practices, into their policies and practices; and specify high-priority gaps for which guidelines, best practices, and new or revised standards are needed and could be addressed by the AI RMF – or which would require further understanding, research, and development.

II. NIST AI RMF – Legislative Initiative: "The American Data Governance Act" with System1, Inc. and Lucd.AI

On behalf of NIST AI RMF, The Team (System1, Inc. and Lucd.AI) has written "The American Data Governance Act" to include the following language supporting NIST's AI Risk Management Framework.

"The American Data Governance Act" addresses American's expectations that Artificial Intelligence and Data Analysis products and services meet common standards based on our collective ideals, norms and values. The American Data Governance Act presents common standards for accuracy, explainability and interpretability, reliability, privacy, safety, security, resilience, and mitigation including bias, diversity and trust. The Act will encompass principles such as transparency, fairness, and accountability during design, deployment, use, and evaluation of AI technologies and systems for National Security. The Act will also set a standard for our Allies to ensure interoperability with the United States."

"The American Data Governance" will create a Digital Public Trust Label for the RMF compliance purpose. For your review, please see the accreditation model to follow highlighting how an AI/ML company and its capabilities can be evaluated and then given a "stamp of standards approval."

III. NIST AI RMF: System1, Inc. and Lucd.AI Providing Responses to Questions 1-12

1. Challenges in AI Management for NIST AI RMF

System1, Inc. and Lucd.AI Response: The Team has identified and understands challenges related to improving how AI actors manage AI-related risks. The term "management" means identify, assess, prioritize, respond to, or communicate those risks and incorporate the management process in the culture for implementation of AI. The challenges for the development and maintenance of the AI risk management framework in priority order are as follows:

- Address the acceleration of AI/ML and quantum capabilities hitting the defense, intelligence. and commercial markets to create a sophisticated secure federated machine learning risk assessment standards platform which can keep up with rapidly evolving technology.
- Improve the AI risk management framework is to have honest conversations about automatous use such as self-driving vehicles for general use, and lethal autonomous weapon systems for counter adversarial threats and attacks.
- Open discussion about the need for privacy and the need for resilience and protection.
- Tailor and create an AI RMF for different sectors. For example, the autonomous vehicle sector is different from the warfighter lethal autonomous weapons sector which is different from our AI/ML chatboxes. Another example would be to discuss with transparency our drones and bring in FAA, TSA, DOT, USAF and USSF.
- Create an AI RMF assessment system which is comprehensive and includes/maps to global risk management/privacy/other related frameworks, like GDPR, ISO, COBIT, to keep up with the evolving AI/ML tools.
- Establish and maintain an ongoing governance process with a Framework assessment accreditation body to keep with applications for certification.
- Promote discussion of human augmentation with AI/ML and Quantum.
- Add ML and Federated Machine Learning and quantum to the RMF title and assessment objectives.
- Strengthen advanced NIST 800-53 cybersecurity protocols within all AI/ML systems.

2. NIST AI RMF Important Characteristics

"How organizations currently define and manage characteristics of AI trustworthiness and whether there are important characteristics which should be considered in the Framework besides: accuracy, explainability and interpretability, reliability, privacy, robustness, safety, security (resilience), and mitigation of harmful bias, or harmful outcomes from misuse of the AI"

System1, Inc. and Lucd.AI Response: All AI/ML and Quantum company employees sign an AI Ethics Code of Conduct (NDA for AI for standards within their organization for Government, Industry and Academia).

3. NIST AI RMF Principles

"How organizations currently define and manage principles of AI trustworthiness and whether there are important principles which should be considered in the Framework besides: transparency, fairness, and accountability"

System1, Inc. and Lucd.AI Response: Our Team is proud to provide data governance, ethics review, data assurance and compliance measures for exceptional analysis and improved situational awareness. We have created "Pillars of Excellence" to include Classified, Regression, Unsupervised, Deep Learning and Explainability. Consistent with the National Security Agency and Intelligence Community Directives for security and privacy, our Team provides a solution which adheres to the Security Technical Implementation Guide, Compliance and a Risk Management Framework, strict Authorization to Operate guidelines, Risk Management Framework guidelines, National Institute of Standards and Technology 501c3, National Institute of Standards and Technology 800-171, the Federal Informational Processing Standard S 2.0, National Institutes of Standards and Technology 80053 Revision 4, International Organization for Standardization 270001, Intelligence Community Directive 503 and the Federal Information Processing 140-2.

The System1, Inc. and Lucd.AI Team provides governance and explainability throughout the machine learning workflow from data management to model serving, including version controls for both modeling and training datasets. This is to support artificial intelligence, governance, and data ingest transformation that could become unstable or lose data integrity.

4. NIST RMF Security Standards

"The extent to which AI risks are incorporated into different organizations' overarching enterprise risk management – including, but not limited to, the management of risks related to cybersecurity, privacy, and safety"

The System1, Inc. and Lucd.AI Response: Our Team's Cybersecurity Standards Include:

1. An on-prem and cloud security solution that operates within the Federal Security Framework – Fed Ramp approved that does Artificial Intelligence and Machine Learning.
2. A Single Sign-on Multi Factor Authentication (SSOMFA) utilizing Central Authentication Service (CAS). CIA & NSA approved and authorized.
3. A Continuous Improvement Plan (CIP) and a Road Map and Quarterly Patching.
4. STIG Compliance and a Risk Management Framework that follows strict ATO guidelines or RMF guidelines NIST 501c3, NIST 800-171, FIPS 2.0, NIST 800-53 Revision 4, ISO 270001, ICD 503, FIPS 140-2.
5. Following guidelines in accordance with SUNNET IL4 government owned network [National Security System].
6. Zero tolerance security, data fusion, large scale ingest, not retaining data, scalability, and infrastructure, utilizing proper security and control mechanisms with these recommendations and role-based authentication and role-based access to ensure data integrity and provide data transformation and data ingest scalability.
7. Security requirements with Accumulo, MAPR, Niagra Files (NIFI), Kubernetes and data modeling to include DASK, Horovod and a Unified Data Space.
8. A Unified Data Space which allows data fusion capable of storing classified / non-classified data with cell-level security.

5. NIST AI RMF Standards

"Standards, frameworks, models, methodologies, tools, guidelines and best practices, and principles to identify, assess, prioritize, mitigate, or communicate AI risk and whether any currently meet the minimum attributes described above"

System1, Inc. and Lucd.AI Response: Our Team adheres to the following principles:

Accountability Principles:

- Build a diverse, well-resourced team to support AI governance and risk management strategy
- Determine with legal the companies' compliance obligations while balancing individuals' rights and freedoms
- Conduct Data Protection Impact Assessment (DPIA) or other impact assessments where appropriate
- Understand the organization's role: controller/processor when using AI systems

Lawfulness, Fairness, Privacy and Transparency of Processing Personal Data:

- Assess statistical accuracy and effectiveness of AI systems in processing personal data
- Ensure all people and processes involved understand the statistical accuracy, requirements and measures
- Evaluate tradeoffs and expectations
- Adopt common terminology that staff can use to communicate about the statistical models
- Address risks of bias and discrimination and work with legal to build into policies

Principles of Security and Data Minimization in AI Systems:

- Assess whether trained machine-learning models contains personally identifiable information
- Assess the potential use of trained -machine learning models
- Monitor queries from API's users
- Consider 'white box' attacks
- and process the minimum amount of data required to achieve the organization's purpose

Compliance with Individual Rights, Including Rights Relating to Solely Automated Decisions:

- Implement reasonable measures respond to individual's data rights requests
- Maintain appropriate human oversight for automated decision-making

6. NIST AI RMF Regulatory Reporting Requirements

"How current regulatory or regulatory reporting requirements (e.g., local, state, national, international) relate to the use of AI standards, frameworks, models, methodologies, tools, guidelines and best practices, and principles"

System1, Inc. and Lucd.AI Response: We will be following NIST 800-53 and ISO to formulate regulatory reporting requirements:

7. NIST AI RMF Principles and Methodologies

AI risk management standards, frameworks, models, methodologies, tools, guidelines and best practices, principles, and practices which NIST should consider to ensure that the AI RMF aligns with and supports other efforts;

System1, Inc. and Lucd.AI Response: Our Team will be following the DC3 Vulnerability Disclosure Program to insure alignment with risk best practices.

8. NIST AI RMF Inclusiveness with Testing and Evaluation

"How organizations take into account benefits and issues related to inclusiveness in AI design, development, use and evaluation – and how AI design and development may be carried out in a way that reduces or manages the risk of potential negative impact on individuals, groups, and society."

System1, Inc. and Lucd AI Response: Our Team is provide a VVE Data Acquisition & Quality Assurance Strategy for the NIST AI RMF. Our Team will provide Testing, Evaluation and Upgrading Capabilities to NIST with unlimited assurance. Our Team is able to provide Operators and Administrators (Data Center, System, Database, Network, Application) responsible to operate all aspects of NIST, including the hardware, network and software with Centralized health monitoring and reporting (agent and agent-less) and Built-in standards-based monitors in all components (custom and COTS) utilizing Distributed file system, Parallelization of logic across nodes, Policy based resource management (prioritization), Elasticity of resources, Throttling, scheduling and Direct attached storage.

9. NIST AI RMF Attributes

"The appropriateness of the attributes NIST has developed for the AI Risk Management Framework.

System1, Inc. and Lucd.AI Response: With thousands of AI/ML and Quantum computing companies developing hundreds of new tools and capabilities each day, the NIST AI RMF needs to have an effective and efficient application, assessment process in place as not to delay evaluations and certifications in near and real time. Standards need to be aligned with accelerated technologies to keep up with market speed and deployment. System1, Inc. and Lucd. AI have built systems with petabyte compute power to handle scale and automation with AI and Federated Machine Learning.

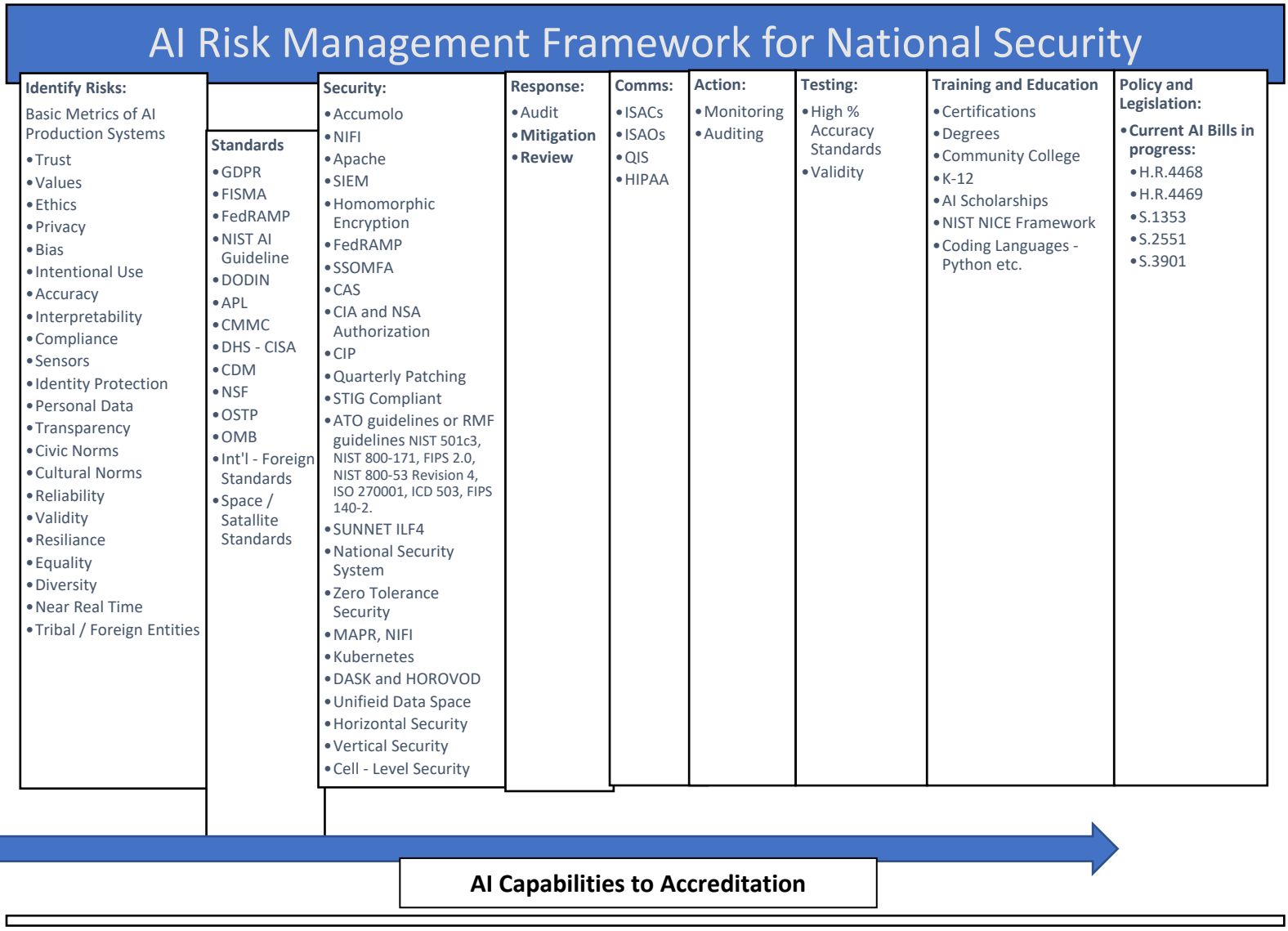
In addition, we bring data in via NSA-developed Niagara Files to ensure we meet govt requirements for scale and performance, but also data governance and provenance. We have extended NIFI to ensure it adheres to the platform Security Model (in this case, for classified data handling), to ensure that data is not only written with the correct security markings, but also within the existing markings in a particular environment (e.g., a TS system may not have a security group for HCS data. The NIFI extensions ensure the logical restrictions of the platform are adhered too, in addition to the correctness).

10.a. Effective Framework Model

"Effective Framework Model"for NIST AI RMF

System 1, Inc. and Lucd.AI Response: Our Team has developed a data analytics platform to support AI/ML and quantum capabilities systems entering into the platform being assessed for risks and standards then measuring security, testing, standards, response auditing and mitigation, communication and information sharing and action like policy, compliance and regulation.

In order to achieve an effective framework for risk evaluation, Lucd AI and System 1, Inc. have developed the below risk assessment model. Please note this AI/ML platform is fully operational and deployed within DOD, IL and the JAIC.

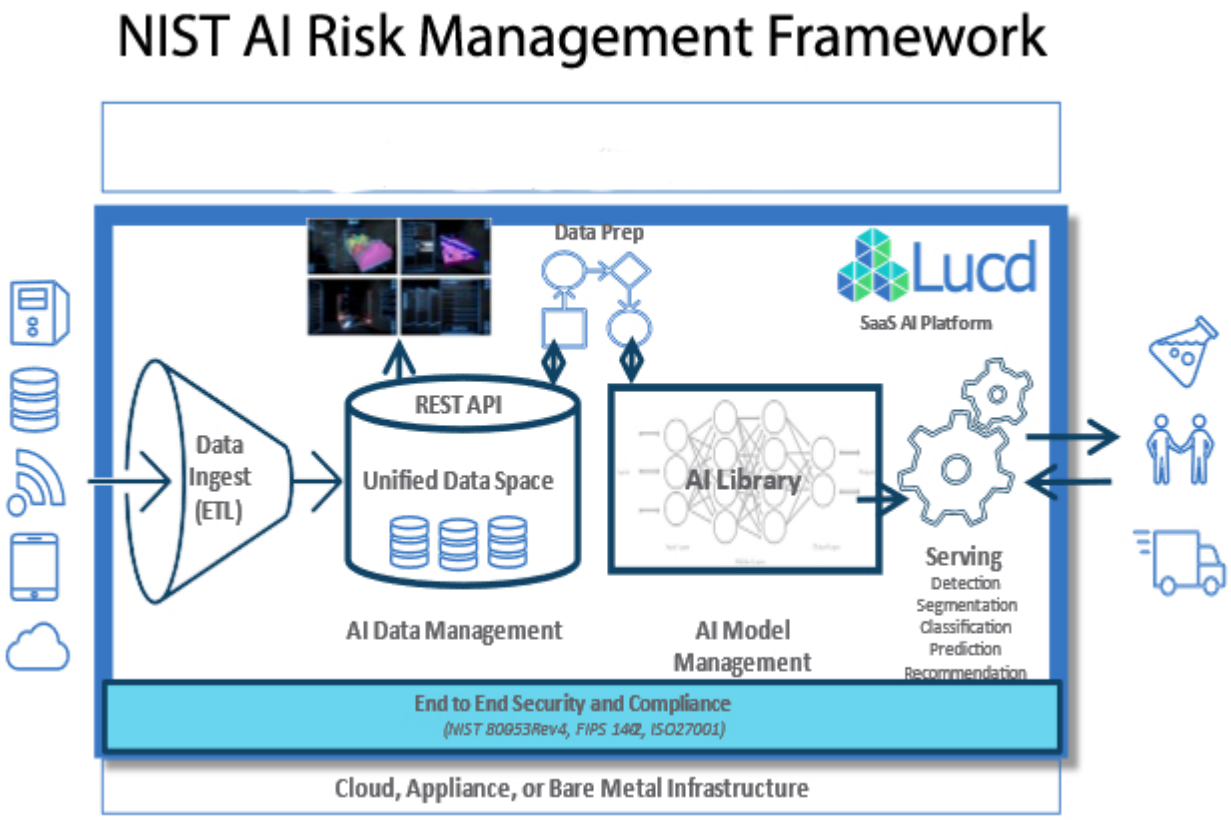


10.b. Effective AI Security Model Framework

In order for AI/ML and Quantum computing data analytic systems to be fully secure, they need to adhere to current NSA, CIA and JAIC National Security protocols. The System1, Inc. and the Lucd AI model highlighted below follows National Security protocols for AI/ML systems. To support the NIST AI Risk Management Framework, AI/ML companies and their capabilities can be assessed with this security data analytics model to insure compliance and accreditation.

Lucd AI together with System 1, Inc. has developed a data analytics platform to support AI/ML and quantum capabilities systems entering into the platform being assessed for risks and standards then measuring security, testing, standards, response auditing and mitigation, communication and information sharing and action like policy, compliance and regulation.

In order for AI/ML and Quantum computing data analytic systems to be secure, current NSA, CIA and JAIC National Security protocols need to be adopted and measured for accreditation using the "Unified Data Space" AI security system described below.



11. NIST AI RMF Workforce Development

"How the Framework could be developed to advance the recruitment, hiring, development, and retention of a knowledgeable and skilled workforce necessary to perform AI-related functions within organizations."

System1, Inc. and Lucd.AI will follow the NIST NICE standards to support a Low-Code No-Code Workforce development framework.

Our Team will install a solution which allows for all levels of operation not only for Subject Matter Experts but for all field engineers in artificial intelligence, machine learning and cybersecurity. The government requires over the shoulder training for Tier I, Tier II - Helpdesk, Tier III and Tier IV for advanced analytics tools to conduct relational, temporal geospatial, statistical network and behavioral intelligence for maximizing predictability, efficiency and model creation and data validation. Our Team will build an immersive experience for all NIST AI RMF users with a multi-player, multi-realm platform supports all levels of training.

In addition to providing subject matter experts in artificial intelligence, machine learning and cybersecurity, we are most proud to educate and train our platforms with an "ease of use" model for all levels of field technicians. On behalf of NIST AI RMF we will enable all teams composed of technical and non-technical roles with a data model system for low-code/no-code and training with robust data in real-time flow across permission levels.

12.NIST AI RMF Governance, Monitoring and Evaluation

NIST AI Governance

System1, Inc. and Lucd.AI Response: Our Team will build a NIST AI RMF to include governance issues, including but not limited to make up of design and development teams, monitoring and evaluation, and grievance and redress. Parallel to evolving approaches used for cybersecurity and development of software a systems security engineering approach should be used during the development as well as agile processes to speed evolution. We provide governance and explainability throughout the machine learning workflow from data management to model serving, including version controls for both modeling and training datasets. This is to support artificial intelligence, governance, and data ingest transformation that could become unstable or lose data integrity.

Our Governance and Explainability is positioned for NIST success. For U.S. NIST AI RMF, we are leading the edge for counter adversarial AI measures. With adversarial analytics, in particular, when the adversary changes either models, data or both, Team engineers have developed an analytic platform with Governance & Explainability (G&E) built in that enables the our client to understand the provenance and pedigree of both data and models in the analytic environment. These include both raw data used to create training datasets, but also **test**, evaluation and inference datasets. Further, both model sources and binaries (trained models) must be included in the G&E workflow to ensure that models remain unaffected by adversaries. We have developed solutions that incorporate homomorphic encryption to ensure that all data being used in the model development process remains encrypted at all times, including in memory.

To follow is a Quad Chart we created for the NIST AI Risk Management Framework:

NIST AI RMF – Risk Factors Evaluation

1.) Trust
2.) Values
3.) Ethics
4.) Privacy
5.) Identity Protection and Personal Data
6.) Bias Review
7.) Diversity Inclusion
8.) Civic Norms/Cultural Norms
9.) International and Foreign Entity Risks
10.) Reliability
11.) Accuracy
12.) Safety Measures
13.) Cybersecurity: homomorphic encryption, NiFi, Accumulo, Cell-Level, SIEM, SIMP
14.) Cyber AI Threats
15.) Adversarial AI: Misinformation/Disinformation
16.) Lethal Autonomous Weapon Systems
17.) Drone Activity CONUS and OCONUS
18.) Compliance
19.) Sensors
20.) Transparency
21.) Accuracy
22.) Explainability
23.) Governance

NIST AI RMF – Standards, Security and Principles

Standards and Principles Evaluated with an Advanced AI/ML Analytic Platform

NIST AI RMF Standards:

1.) NIST AI Guidelines
2.) FISMA
3.) FedRamp
4.) DODIN
5.) CMMC
6.) APL
7.) COM
8.) GDPR

NIST AI RMF Security Architecture Controls:

- JAIC 4,5 IL Approved
- Accumulo, MAPR, Niagra Files, Kubernetes and Cell Level security with SUNNET IL-4 National Security Approved
- AI Horizontal and Vertical security controls
- AI Secure with NIPR, SIPR, JWICS, BICES and DREM
- NIST AI Security Guidelines

NIST AI RMF Principles:

1.) Transparency
2.) Fairness
3.) Accountability

NIST AI RMF – Communication

- Information Sharing (ISACS)
- Sector AI RMF Review Boards: DOD, USSF, Energy, Finance, Insurance, Pharma, Bio-Tech, FEMA, DOT
- Mitigation, Auditing, Regulations, Policy and Laws
- Education and "AI Training for ALL" and "Analytics Anywhere"
- Lo-Code and No-Code: Easy analytic tools for all users
- Collaboration

NIST AI RMF - Outcomes

- AI RMF Analytic Standards Model
- AI RMF Guidelines
- AI RMF Best Practices
- AI RMF Methodologies
- AI RMF Tools to Manage Risk Adoption
- AI RMF Evaluation
- AI RMF Accreditation, Certification
- AI RMF Testing
- AI RMF Education
- AI RMF Training
- AI RMF Public Library/Resources
- AI RMF Policy, Regulation and Laws

IV. References

Lucd AI and System 1, Inc. referred to the following references in compilation of this document:

- Readout of the First National Artificial Intelligence Research Resource Task Force Meeting, July 29, 2021
- National Artificial Intelligence Research Resource Task Force (NAIRR TF), May 2021
- Biden Administration launches the National Artificial Intelligence Research Resource Task Force, News Release 21-006
- National Artificial Intelligence Initiative, May 2021
- 2016-2019 Progress Report: Advancing Artificial Intelligence R&D, November 2019
- NSF leads federal partners in accelerating the development of transformational, AI-powered innovation, Oct. 8, 2019
- The National Artificial Intelligence Research and Development Strategic Plan: 2019 Update, June 21, 2019
- Artificial Intelligence Past and Present, June 24, 2019
- NSF joins federal partners in announcing update to national AI research and development strategic plan, June 21, 2019
- Statement on executive order to maintain American leadership in artificial intelligence, Feb. 11, 2019
- Executive Order on Maintaining American Leadership in Artificial Intelligence, Feb. 11, 2019
- Comments Received in Response to the Request for Information on Update to the 2016 National Artificial Intelligence Research and Development Strategic Plan, Dec. 19, 2018
- Update from the NSTC Select Committee on AI, Nov. 30, 2018
- Request for Information on Update to the 2016 National Artificial Intelligence Research and Development Strategic Plan, Sept. 26, 2018
- A New NITRD IWG for AI R&D, July 2, 2018
- Summary of the 2018 White House Summit on Artificial Intelligence for American Industry, May 10, 2018
- Statement on Artificial Intelligence for American Industry, May 10, 2018
- Testimony of Dr. Jim Kurose, CISE AD, before the Subcommittee on Information Technology for the Committee on Oversight and Government Reform, U.S. House of Representatives, March 7, 2018
- Remarks of Dr. France Córdova, NSF Director, at the NVIDIA GPU Technology Conference, November 1, 2017
- Remarks of Dr. France Córdova, NSF Director, at the NVIDIA GPU Conference, Oct. 26, 2016
- NSF statement of support for National Artificial Intelligence Research and Development Strategic Plan, Oct. 26, 2016
- The National Artificial Intelligence Research and Development Strategic Plan, Oct. 2016