NEC Corporation of America
1820 North Fort Myer Drive, Suite 400
Arlington, VA 22209

September 15, 2021

**BY ELECTRONIC MAIL**
Mr. Mark Przybocki
Division Chief, Information Access Division
U.S. National Institute of Standards and Technology, MS 20899
100 Bureau Drive
Gaithersburg, MD 20899

**Re: Docket No. 210726-0151: NEC Corporation of America Comments on the National Institute of Standards and Technology's Proposed AI Risk Management Framework**

Mr. Przybocki:

NEC Corporation of America ("NEC") is pleased to submit comments in response to the Request for Information ("RFI") regarding the Artificial Intelligence Risk Management Framework (AI RMF) that the National Institute of Standards and Technology (NIST) is developing.[1] Specifically, NIST is seeking information on "how individuals, groups and organizations involved with designing, developing, using, or evaluating AI systems might be better able to address the full scope of AI risk and how a framework for managing AI risks might be constructed."

As a key member of the information technology industry and a major global supplier of biometric technologies and other AI solutions, NEC appreciates NIST's consensus-driven, transparent approach to building a flexible, adaptable, and understandable framework for mitigating the risks that AI technologies can pose throughout their lifecycles. NEC recognizes that AI technologies, which frequently provide significant benefits to individuals and societies around the world, can sometimes perpetuate harmful biases and discrimination and pose risks to individual privacy and other civil and human rights. We are committed to building digital trust by producing AI solutions that are reliable, secure, and supportive of human rights and social justice, and we support NIST's efforts to develop its AI RMF and advance broader trustworthy AI.

We respectfully submit these comments to share information pertaining to several topics in the RFI, including:

- How organizations currently define and manage characteristics and principles of AI trustworthiness;
- The integration of AI risk management into broader enterprise risk management;
- Existing standards, frameworks, models, methodologies, tools, guidelines, best practices, and principles to identify, assess, prioritize, mitigate, or communicate AI risk;

[1] *See* National Institute of Standards and Technology, *Artificial Intelligence Risk Management Framework*, 86 FR 40810, Docket No. 210726-0151 (rel. July 29, 2021) ("Public Notice"), .

- How organizations take into account benefits and issues related to inclusiveness in AI; and
- How to structure NIST's AI RMF in order to help achieve the desired goals.

## I. Overview of NEC and Our AI Solutions

Headquartered in Irving, Texas, NEC (https://www.necam.com/) is a subsidiary of NEC Corporation, a global technology firm with $28 billion in annual revenue, a presence in over 160 countries and regions, and more than 110,000 employees worldwide. NEC Corporation has had a presence in the United States since 1963, and, today, our major U.S. offices span sixteen states and employ over 2,000 people. One of the world's top patent-producing companies, NEC Corporation combines advanced technologies, services, knowledge, and its 120 years of operating experience to help promote safety, security, fairness, and efficiency and build a more sustainable world in which all people have the opportunity to reach their full potential.

NEC delivers one of the industry's strongest and most innovative portfolios of biometrics, security, analytics, and information and communications technology (ICT) solutions for enhanced customer experience, safety, and productivity. NEC National Security Systems (NSS) launched in 2020 as a wholly owned subsidiary of NEC Corporation of America and will operate under an anticipated Special Security Agreement (SSA) with the U.S. Government as a FOCI-mitigated entity. NEC NSS provides U.S. Government customers with access control, identity verification, scene processing, advanced analytics, fiber optic sensing, border control, and transportation security solutions. Throughout the United States and around the world, NEC also implements, deploys, and supports large-scale information technology, communications, and AI solution integrations that perform mission-critical services for commercial customers, state and local law enforcement agencies, and other public-sector customers.

Below, we describe applications that incorporate several of our AI technologies, including System Invariant Analysis Technology (SIAT), RAPID Machine Learning (RapidML), Heterogeneous Mixture Learning (HML), and biometric technologies.

### *A. System Invariant Analysis Technology*

Early failure detection is challenging with conventional threshold monitoring, but SIAT helps prevent system failures, improve system availability, and reduce maintenance costs. SIAT is an analytics engine that gathers and analyzes sensor data from buildings, factories, power plants, bridges, tunnels, and other infrastructure and machine environments. Leveraging the power of white-box AI, NEC's SIAT solutions facilitate predictive maintenance by monitoring invariant relationships among sensors and detecting anomalies that could signal an impending malfunction. Monitoring performance of individual machines can also help engineers model broader system operations, which can make planning overall machine operations more efficient and effective.

Among our most notable SIAT deployments is NASA's use of SIAT in the Orion spacecraft building and testing processes. During the Orion capsule thermal vacuum testing, SIAT helped process data from nearly 150,000 spacecraft sensors and produce an exhaustive, holistic, analytical model that incorporated over 22 billion data relationships and helped model nominal operations and detect irregularities.

In the future, NEC aims to expand the use of SIAT from servers to edge and embedded computing platforms. We are also working to incorporate SIAT into post-flight aircraft inspections, satellite ground stations, and reusable rocket systems.

### *B. RAPID Machine Learning*

NEC's RapidML is a high-speed deep learning technology that enables high-precision image classification and matching by automatically extracting data features, such as images, text, and numbers, and analyzing those features in a manner that reduces manual analysis requirements. RapidML can help facilitate faster and more accurate manufacturing defect inspection by recognizing a wider variety of defects than conventional machine vision techniques. Because RapidML can detect defects on diverse surfaces, it is highly adaptive and useful in a range of manufacturing industries.

### *C. Heterogeneous Mixture Learning*

NEC's HML learns multiple relationships in big data, automatically discovers useful patterns and regularities, and makes predictions by selecting the appropriate pattern for the situation. Compared to other machine learning technologies that often take just a single pattern into account, HML's use of multiple patterns enables higher-precision predictions in dynamically changing environments. Moreover, our white-box AI approach helps make these predictions explainable. By making more precise, explainable predictions, HML technologies can help improve demand forecasting, thereby improving production and distribution efficiency and reducing shortages and waste.

### *D. Biometric Technologies*

NEC's biometric technologies help identify individuals and/or analyze individuals' characteristics based on their physical attributes, such as their faces, irises, fingerprints, palm prints, voices, gaits, or body temperatures. We have invested significant resources in research and development, and our state-of-the-art AI/ML technology has helped us provide a variety of customers with biometric algorithms that are among the world's fastest and most accurate across demographic groups and other challenging use cases. We began our biometrics business as a leading provider of Automated Fingerprint Identification Systems (AFIS) to state and local law enforcement agencies, and we built on our law enforcement expertise to become a trusted biometric technology provider to the U.S. federal government. We also provide commercial customers in the aviation, health care, entertainment, financial services, and hospitality industries with a variety of unimodal and multimodal biometric solutions.

## II. <u>NEC Practices to Promote Responsible, Trustworthy AI</u>

### *A. NEC's Corporate Structure Helps Mitigate AI Risks and Maximize AI Benefits.*

NEC Corporation works to incorporate Environmental, Social, and Governance (ESG) initiatives into our worldwide corporate practices. Specifically, NEC Corporation works to build safer cities and promote innovation throughout the value chain by taking actions to address climate change, strengthen privacy policies and implement other measures aligned with societal expectations, heighten security to maximize ICT possibilities, and develop sustainably and socially literate human resources.

NEC Corporation's Digital Trust Business Strategy Division (DTBSD) works with the Corporate Communication and Sustainability Promotion Divisions on several of these ESG initiatives and leads ongoing efforts to formulate and implement a strategy for promoting human rights in our biometrics and broader AI business. Throughout the course of developing and implementing the global human rights promotion strategy, DTBSD consults diverse experts about human rights issues relevant to our business and to the communities in which we operate. Furthermore, to improve and manage company-wide privacy and human rights policies and programs, DTBSD collaborates with other internal teams worldwide, including the People and Organization Development Division, global quality management and cybersecurity teams, and regional subsidiary teams that are working to build digital trust in their local markets.

In the United States, NEC takes a three-pillared approach to building digital trust by promoting (1) **reliability**, (2) **ethics and human rights**, and (3) **security** in our business practices, services, and technologies. The NEC Digital Trust Working Group strives to coordinate with the Diversity, Equity & Inclusion Steering Committee, Creating Social Value Task Force, and the NEC Foundation to align objectives and effectively leverage resources to strengthen all of our U.S. ESG initiatives.

### ***B. NEC Promotes AI Reliability with Quality and Safety Management and Third-Party Testing.***

Our approach to AI reliability is integrated into our broader safety and quality management initiatives that help promote reliability throughout NEC's supply chain and in product design, development, and deployment. NEC Corporation works with NEC and other subsidiaries to hold semi-annual quality promotion meetings and implement the "Quality and Safety Action Policy." These efforts aim to help prevent product defects, facilitate compliance with worldwide quality and safety laws and regulations (including consumer protection laws in Japan, Britain, and Canada), encourage internal teams to share expertise, and standardize practices and key technology components. The "NEC Group Procurement Policy" underscores NEC's commitment to procuring quality goods and services under fair business terms. Additionally, NEC Corporation has been working to create Environment and Total Quality Management Divisions in each business unit and consolidated subsidiary and to have each business unit and subsidiary appoint a Quality and Safety Management Officer.

To address quality management issues specific to AI technologies, NEC Corporation developed "Guidelines to Quality Assurances for Machine-Learning-Based AI." These guidelines aim to go beyond traditional software quality assurance guidelines and help data analysts across NEC Corporation companies better understand the processes behind machine learning and other forms of AI analysis.

Furthermore, NEC seeks out opportunities to submit our AI solutions to independent, third-party testing to help validate and improve their performance. For example, to obtain independent evaluations of our biometric algorithms' accuracy overall and across demographic groups and other challenging use cases, NEC has been participating in NIST vendor tests for over a decade. NEC also participates in U.S. Department of Homeland Security (DHS) Science and Technology Directorate (S&T) Biometric Technology Rally testing. We are proud to have consistently ranked among the top providers of fingerprint, iris recognition, and face recognition algorithms.

In addition to this recognition from NIST and DHS S&T, NEC Corporation is proud to have received several other global awards producing innovative, high-quality, and high-performing AI technologies. In recognition of NEC's pivot toward biometric solutions beyond traditional biometric markets and NEC's dedication to creating new customer cases and enhancing customer solutions, NEC received the 2020 Global Biometrics in Security Market Growth Innovation & Leadership Excellence Frost Radar$^{TM}$ Award from Frost & Sullivan. Additionally, NEC's "Smart Airport" technology won the Service Design iF DESIGN AWARD, and our "Walking Analysis Technology" won the Healthcare iF DESIGN AWARD. From 2011 to 2020, NEC received the Top 100 Global Innovator Award from Clarivate Analytics for Hardware & Electronics. In 2019, Frost & Sullivan named NEC as the Asia Pacific Biometric Company of the Year.

### *C. NEC Promotes Ethical, Secure AI by Operationalizing our AI and Human Rights Principles.*

In 2018, DTBSD led the effort to develop NEC Group AI and Human Rights Principles, which promote: (1) fairness; (2) privacy; (3) transparency; (4) responsibility to explain the effects, value, and impacts of AI utilization; (5) proper utilization of AI technology; (6) continued development and improvement of AI technologies; and (7) dialogue with multiple stakeholders.

We are committed to upholding our AI and Human Rights Principles, and we have already started to operationalize these Principles through our corporate governance, AI product risk management, customer and partner relationship management, and our internal and external multi-stakeholder engagements.

#### 1. Corporate Governance

The NEC Corporation Privacy Policy and personal information protection management system mandate handling personal information in accordance with the requirements in Japan's Act on the Protection of Personal Information and JIS Q 15001, the Japanese industrial standard for safe and appropriate management of personal information in corporations' and other organizations' operations. We have also developed and implemented data breach response procedures to help ensure that, if a data breach does occur, we are well positioned to respond effectively and in a manner that minimizes harm to the individuals whose personal information we retain.

NEC Corporation first earned our PrivacyMark certification in October 2005. To earn the PrivacyMark certification, companies must comply with JIS Q 15001 and gain third-party organization recognition for having systems in place to ensure appropriate protection measures for personal information. The PrivacyMark certification also prohibits companies from collecting information that could economically impact an employee, such as bank account and credit card information; sensitive information, such as birthplace; or highly private information, such as a mobile telephone number, without obtaining consent. As of March 2021, NEC Corporation and thirty of its affiliated companies hold the PrivacyMark Certification.

Furthermore, throughout the AI product lifecycle, NEC prioritizes observability and traceability, meaning that we monitor our AI's performance and compare actual performance to intended performance.  Our Artificial Intelligence Operations and Machine Learning Operations teams help ensure we take appropriate actions to address any biased, unreliable, or otherwise unintended AI predictions before we finish developing and start deploying our AI technologies.

### 2. AI Product Risk Management

Our approach to AI product design and development occurs in three stages: visualization, analysis, and prescription.  The visualization stage involves digitizing information from the real world.  During the analysis stage, we analyze and predict the background and future of the data we obtained through visualization.  In the prescription phase, we plan and implement the best solutions for any issues we foresee.

Throughout all three phases, we work to mitigate technical risks.  Technical risks may arise due to a variety of issues, including poor quality data, data misinterpretation, ineffective feature engineering, insufficient modeling, and adversarial attacks.  If our testing and evaluation demonstrates that an AI technology is producing unreliable or unfair results, we work to retrain the technology.  Often, our retraining process involves focused efforts to improve our AI technology's performance on particularly challenging use cases.  For example, while NEC was working on one of its initial face recognition technology aviation projects, we noticed that the face recognition technology was less accurately identifying individuals with facial hair.  To address this problem, we retrained the algorithm using training data that specifically helped the algorithm learn to more accurately identify individuals with facial hair.  Employing a similar retraining approach after testing on other challenging use cases, like demographic groups, has helped NEC's algorithms achieve top performance in NIST Face Recognition Vendor Test (FRVT) reports that specifically focused on assessing face recognition algorithm performance across age groups and demographic groups based on race and sex.

Moreover, throughout the product design and development process, NEC promotes privacy and fairness by leveraging safeguards such as encryption, data minimization, data aggregation, data anonymization, and algorithm layering.  In addition to producing traditional "black-box" AI solutions, we also work to design transparent and explainable white-box AI solutions.  These white-box AI solutions provide greater insight into why the AI technology produced a certain result, which makes them especially useful in use cases for which there is more than one possible "right" answer.

### 3. Customer and Partner Relationship Management

Before selling our highest-risk AI solutions through new partners and/or to new customers, we think that considering the prospective partners' and customers' human rights records and risk mitigation policies is important.  We aim to sell only through trusted partners and to trusted customers, and we are willing to decline business opportunities that we determine may pose too great a risk to human rights.

After we decide to sell an AI solution to a customer, we work with the customer (and, if applicable, the partner(s)) to plan and execute deployments and to train individuals operating the AI systems.  We recommend that end users require human review of important algorithm match results and continuously monitor system performance, and we provide operators with ongoing support via a customer service helpline and field site visits.

We also work with our partners and customers around the world to facilitate multijurisdictional compliance.  We also work with partners and customers to consider ethical issues that may arise in the context of the customers' AI technology deployment, and our consideration of these ethical issues reflects perspectives gained through collaboration with diverse internal and external stakeholders.

### 4. Multi-Stakeholder Engagement

We are actively working to strengthen human rights literacy and promote diversity, equity, and inclusion (DEI) throughout NEC, and particularly on our AI teams.  In addition to providing training programs and advancing other education and information sharing initiatives, we recognize the importance of continuing to deepen collaboration between our DEI Steering Committee, our Digital Trust Working Group, and our broader product and leadership teams, so that we can more completely embed our commitments to DEI and social justice into our policies, programs, and practices for designing, developing, deploying, and evaluating our AI technologies.

To inform our perspectives and positions on issues at the intersection of AI and human rights, we also participate in dialogues with a wide array of external stakeholders, including policymakers, civil society organizations/NGOs, think tanks, industry groups, end user groups, and academic researchers around the world.  In the United States and internationally, we actively engage with national and international organizations that work on developing standards and ethical guidelines for AI technologies, including the Biometrics Institute, Security Industry Association, International Biometrics + Identity Association, U.S. Chamber of Commerce, Future of Privacy Forum, World Economic Forum, United Nations, and standards bodies like NIST.  We also welcome opportunities to serve as a resource to policymakers and other stakeholders who are interested in learning more about how our AI technologies work and in developing approaches to mitigating AI risks while realizing AI benefits.

## III. Characteristics of Effective AI Governance and Risk Management Frameworks

We believe that governance frameworks for AI technologies should reflect input from diverse stakeholders and should be use-case-specific, risk-based, and supportive of privacy and other civil rights and civil liberties, racial and broader social justice, safety, security, economic efficiency, and technological innovation.

Some of the most effective AI governance frameworks that we have seen proposed and adopted require appropriate and feasible notice and consent to data collection and the use of AI technologies; strong cybersecurity protections; limitations on data handling, storage, retention, and transfer; independent, third-party testing before and after deploying the AI systems; operator training; public reporting and oversight to the degree appropriate for various use cases; meaningful human review of high-stakes algorithm outputs; prohibitions on discrimination in decision-making based on AI outputs; and use limitations to ensure existing constitutional protections appropriately demarcate uses of AI technologies in the United States.

Although several groups have already developed principles, guidelines, best practice recommendations, legislative proposals, and other types of governance frameworks to help mitigate AI risks and realize AI benefits, NEC would appreciate additional input from NIST. Guidance regarding the technical dimensions of AI risk management during each stage of the AI lifecycle would be particularly helpful.

As NIST continues advancing its important AI RMF initiative and related trustworthy AI efforts, NEC welcomes future opportunities to support NIST's work and provide any further input and assistance that would be helpful.

Sincerely,

S. Takahashi

Shin Takahashi
Chairman and Head of Government Relations