# PUBLIC SUBMISSION

**Received:** May 23, 2025
**Tracking No.** mb1-3aa7-yft6
**Comments Due:** May 28, 2025 **Submission Type:** Web

**Docket:** NSF-2025-OGC-0001
NITRD_FRDOC_0001

**Comment On:** NSF-2025-OGC-0001-0001
Request for Information: Development of a 2025 National Artificial Intelligence Research and Development Strategic Plan

**Document:** NSF-2025-OGC-0001-DRAFT-0100
Comment on FR Doc # 2025-07332

## Submitter Information

**Organization:** Infineon Technologies Americas Corp

## General Comment

Thank you for the opportunity to comment on development of the National Artificial Intelligence Research and Development Strategic Plan. Attached please find the comments of Infineon Technologies Americas Corp. Best, Maria DiGiulian, Senior Director, Government Relations.

## Attachments

2025 05 29 RFI on AI RD Strategic Plan_Infineon FINAL

**Request for Information on the Development of a 2025 National Artificial Intelligence (AI) Research and Development (R&D) Strategic Plan, Networking and Information Technology Research and Development (NITRD) National Coordination Office (NCO), National Science Foundation**

Submission by Infineon Technologies Americas Corp.
Contact: Maria DiGiulian, Senior Director, Government Relations, Infineon Technologies Americas Corp.
Due Date: May 29, 2025
Docket ID No. NSF-2025-OGC-001

## Introduction

Thank you for the opportunity to provide comments to the "Request for Information on the Development of a 2025 National Artificial Intelligence (AI) Research and Development (R&D) Strategic Plan."

There are four key issues that Infineon Technologies Americas Corp. (Infineon Technologies) respectfully requests the U.S. government consider in forming an AI R&D Strategy.

1. Prioritize research to advance compute efficiency for aerospace and defense capabilities
2. Prioritize research to advance encryption, anomaly detection, and automated response systems
3. Prioritize research of magnetics and passives and advanced packaging
4. Collaborate with like-minded allies and partners to address global challenges in AI research, advance common goals, and drive forward and strengthen world class research and innovation

Focusing on these topics will help the U.S. government achieve its goals in AI, AI infrastructure, aerospace and defense, security, and other areas.

## Infineon Technologies AG

Infineon Technologies AG is a global semiconductor leader in power management systems and the Internet of Things. It is the number one global supplier of semiconductors to the automotive industry and is number one in the global microcontroller market. Infineon is also a leader in wide band gap semiconductor materials such as gallium nitride (GaN) and silicon carbide (SiC), which allows semiconductor power devices to operate at higher voltages, temperatures, and frequencies. It offers the broadest product and technology portfolio in wide band gap devices. Infineon serves the automotive, industrial, energy, and AI sectors. The company has approximately 58,000 employees worldwide and generated revenue of about €15 billion in fiscal year 2024 (about $15.7 billion U.S. dollars). Infineon is listed on the Frankfurt Stock Exchange (IFX) and in the United States on the OTCQX international over-the-counter market (IFNNY). Infineon Technologies is

headquartered in Munich Germany, with its U.S. operations headquartered in San Jose, California. It has a large U.S. presence including fabrication and R&D facilities in 12 states.

Infineon partners with the U.S. government through the USA Manufacturing Institute PowerAmerica, multiple NASA programs, the Air Force Research Lab, DARPA and other defense departments, and ARPA-E. Infineon was awarded the Trident II flag for its support of the U.S. Navy. It also supplies the security chips and modules that protect the U.S. passport and has reached a milestone of supplying over 270 million of those secure chips.

## Infineon Technologies and Artificial Intelligence

Artificial Intelligence is the transformative technology of our time. From manufacturing to retail, healthcare to automotive, the ability of computer systems to perform cognitive functions that have traditionally only been associated with humans - such as perceiving, reasoning, problem-solving and learning - is having an incredible effect across multiple sectors and will be felt anywhere and everywhere in our daily lives.

This rapidly evolving landscape profoundly affects the entire supply chain as component and system suppliers become enablers of future high-performing, energy-efficient and reliable AI applications. The semiconductor industry, in particular, plays an essential role in this development - because AI applications are based on semiconductor solutions such as advanced sensors, microcontrollers, accelerators and memory solutions. The semiconductor industry, powered by AI technology, is ideally positioned to serve as a prime catalyst for driving future advances in AI deployment.

As AI applications evolve, they become more comprehensive, complex, and application specific. While software brought the first development pushes in AI, and hardware formed the basis of initial advances, the parallelism of hardware and software development will enable the next major AI breakthroughs, as the complexity of algorithms and computational models requires new performance dimensions of the associated technical components.

AI models also require substantial computational power for training and inference, making them incredibly energy hungry. The growth of AI will, therefore, drive increased demand for data center capacity that must be met through technologies that improve power efficiency, performance, and reliability. An energy-efficient and top-performing power supply is essential for AI data centers, and the industry as a whole must minimize energy consumption, reduce costs, manage heat, and ensure reliability.

For companies such as Infineon, these factors present exciting opportunities to enable the rapid deployment of AI solutions across markets. That said, industry needs key government focus and support in specific areas to unleash this AI revolution.

1. **Prioritize Research to Advance Compute Efficiency for Aerospace and Defense Capabilities**

One key AI R&D focus area for the United States, particularly in the defense context, is research in edge AI applications that increase compute efficiency – a focus area critical to maintaining leadership and an effective, modern defense.

AI applications are moving from the cloud to the device, or the "edge." Edge AI devices are *critical* for enabling warfighters to deploy autonomous applications in harsh combat environments. These specialized systems can process data locally without connectivity to central networks, which allows for real-time decision-making while maintaining operational security and reliability under extreme conditions where power sources may be limited or unreliable. The ability to operate in areas with no connectivity is particularly vital. Warfighters often conduct missions in remote or contested regions where communication infrastructure is damaged, jammed, or nonexistent. These operations simultaneously face environmental challenges such as extreme temperatures, dust, moisture, and radiation, and physical impacts that conventional computing systems cannot withstand.

Applications like automated threat detection through compact sensor fusion systems, tactical drone swarm coordination, and AI-powered battlefield situational awareness tools enable soldiers to maintain decisive advantages without compromising mobility or increasing their electromagnetic signature in contested environments. Furthermore, real-time processing capabilities in space applications, particularly onboard satellites, can be instrumental for immediate threat detection, surveillance, and mission support, eliminating transmission delays and reducing vulnerability to communication disruptions while providing critical intelligence directly to forward-deployed units. These real-time processing capabilities are vital to the Golden Dome project, ensuring rapid, autonomous decision-making in space to enhance national security and operational effectiveness.

Focusing R&D efforts in this area is vital to maintaining modern aerospace and defense capabilities.

## 2. Prioritize Research to Advance Encryption, Anomaly Detection, and Automated Response Systems

The rapid proliferation of AI-based software has revolutionized industries such as healthcare, transportation, cybersecurity, and finance, driving significant technological progress. However, this growing dependence on AI systems also creates new vulnerabilities that malicious actors can exploit. A successful attack on these systems could lead to severe consequences, including data breaches, financial losses, or even physical harm. Consequently, the U.S. government should prioritize the security of AI systems within the broader framework of cybersecurity risk management, addressing the unique threats these technologies face. One key area of focus could be R&D to advance encryption, anomaly detection, and automated response systems to keep pace with evolving threats.

While much of the current discourse surrounding AI centers on issues like bias, trustworthiness, and ethical implications, the security of AI itself demands equal attention. AI-specific threat vectors, if left unaddressed, could heighten risks to national security and public safety.

Fortunately, both public and private sectors can adopt established best practices to bolster the security of AI systems. As the complexity of security challenges grows, particularly with the shift toward edge devices, safeguarding AI becomes even more critical. Edge devices, which process data locally rather than in the cloud, are especially vulnerable to tampering, malicious updates, and breaches in data path integrity. Securing AI at the edge is essential for the operational safety of these devices and for protecting user privacy and has major national security implications for the military uses of edge AI.

In data centers, hardware security provides a foundational layer of protection, leveraging technologies like Trusted Computing, isolated processing, and cyber resilience. These well-established tools are widely implemented and form a robust base for secure infrastructure. Nevertheless, as adversaries refine their techniques, ongoing research is necessary to stay ahead of emerging threats.

Similarly, AI-enabled sensors, designed for remote data analysis and enhanced privacy, offer significant benefits but can become entry points for malicious activity if not properly secured. These sensors, which perform AI tasks in isolated environments and minimize data transmission, enhance security by reducing exposure. However, vulnerabilities in their AI functions can still be exploited, posing risks to both individual devices and broader systems.

AI-enabled sensors face three primary types of threats that require mitigation. First, tampering with the AI model on the device can lead to incorrect decisions, potentially granting unauthorized access or blocking legitimate users. Second, malicious software or firmware updates can compromise the sensor's functionality. Third, maintaining the integrity of the data path from the sensor to its output is crucial because intercepted or altered data could subtly skew outcomes in ways undetectable to humans. For instance, a compromised AI-enabled camera on a smart lock could allow unauthorized entry by accepting a spoofed profile, or it could deny access to legitimate users, effectively creating a new form of distributed denial-of-service (DDoS) attack.

The risks associated with AI-enabled sensors extend beyond individual devices to entire systems. For example, a tampered camera in a smart home could unlock doors for intruders by injecting falsified images, or it could block specific individuals, denying them entry across multiple access points. These vulnerabilities also apply to public spaces, buildings, and infrastructure where AI sensors manage access privileges. Beyond access control, AI models that regulate traffic flow based on camera feeds are equally susceptible. If tampered with, these systems could disrupt traffic patterns or cause accidents, highlighting the broader implications of unsecured AI.

These security challenges are not unique to camera-based systems; they also inform other applications, such as voice-controlled access or autonomous vehicles, which rely heavily on computer vision and sensor data. A breach in any of these contexts could have cascading effects, undermining safety and trust in AI technologies.

As quantum computing technology advances, post-quantum cryptographic algorithms become increasingly essential. After a multi-year process, NIST has agreed on several such algorithms but some of their characteristics (e.g., longer keys and signatures) present challenges for the small

embedded systems that are often used in AI-enabled sensors. Thus, further research is needed into methods for implementing post-quantum cryptographic algorithms in embedded systems.

To fully address AI security into the future, we respectfully recommend that funding and prioritizing research for AI security, including cybersecurity solutions, for AI. As AI continues to permeate critical sectors, securing these systems is not just a technical necessity but a national priority. Research areas could include:

- Development of predictive AI models to forecast potential cyberattacks, enabling proactive measures to strengthen digital resilience;
- Advancement of AI-driven technologies, such as encryption, anomaly detection, and automated response systems to keep pace with evolving threats.

3. **Prioritize Research to Advance Magnetics and Passives and Advanced Packaging**

To continue to move forward with innovation solutions for making power use more efficient for AI, and specifically in data centers, there are specific areas in which the United States should increase its investment in research and development: magnetics and passives, as well as advanced packaging.

With high density power solutions needed to meet the energy requirements of datacenters, magnetics and passives, as well as advanced packaging to include chiplets, 3D packaging, and embedded silicon substrates, will play an increasingly important role in efficient system design. To date, significant amounts of this work is done in Asia, and there are few companies focused on innovating and manufacturing inductors, transformers, capacitors, and connectors in the United States. Magnetics are increasingly becoming a bottleneck. Thermal design faces the same issues with innovation and manufacturing focused in Asia.

There is a clear need for innovation in these areas in the United States to maintain the lead in powering AI.

**4. Collaboration with Like-Minded Countries**

Collaboration with like-minded countries provides significant benefits and supports U.S. leadership in AI. International collaboration can address shared interests in global national and economic security challenges that AI development faces. It also facilitates R&D to improve access to essential technologies. R&D collaboration with like-minded countries can advance common goals and provide access to international scientific capabilities, technologies, and advancements, thereby accelerating innovation. It provides an innovation ecosystem that shares costs, resources, and expertise to expand the impact of U.S. R&D investments, technologies, and scientific leadership.