Implementing Security Technologies for Organizational Security Governance through the National Network Security Framework (N²SF)

1. Introduction

In response to the increasing cyber threats, the government is shifting its security paradigm by introducing the **National Network Security Framework (N²SF)**. This report outlines the background of the N²SF initiative, its phased development, international trends, and future directions for implementing security technologies to realize organizational security governance.

---

2. Evolution of National Network Security Policies

2.1 Initial Policy Phase

- **2006**: The mandatory network separation policy was announced, followed by the first project involving 18 government agencies.
- **2008**: The second phase expanded to 27 additional agencies.
- **2010**: The National Intelligence Service revised the policy, emphasizing the need for improving the national network security framework.

2.2 Framework Enhancement and Transition

- **2014–2020**: With the enactment of the Cloud Development Act and challenges such as COVID-19, a joint public-private task force was established to advance security policies.
- **2021 onwards**: A roadmap for the transition to N²SF was developed, detailing principles, application procedures, and security measures.
- **2024–2025**: Security guidelines have been published in draft form and are expected to be finalized in version 1.0.

---

3. N²SF Security Classification and Application

N²SF is based on a **three-tier data classification system** to ensure differentiated protection.

- **Classified (C)**: Core information related to national security, diplomacy, and defense.
- **Sensitive (S)**: Personal or business-related sensitive information.
- **Open (O)**: All other information outside the classified or sensitive categories.

This classification provides the foundation for data handling policies across organizations, particularly in cloud and AI environments.

---

4. International Developments

- **United States, Australia, and Canada** are building **classified cloud systems** to manage national confidential data.
- The U.S. government requires cloud service providers (CSPs) to deliver highly reliable technologies, while the EU promotes safety through frameworks such as the **AI Act** and **AI RMF**.
- Major countries are investing in **AI security control technologies** to enable safe AI utilization within classified networks.

---

5. AI-Driven Security under N²SF

N²SF is designed to secure diverse forms of national data.

- **Data types**: Documents, images, audio, and more.
- **Implementation**: AI-driven controls are applied with differentiated security levels in classified cloud environments.
- **Objective**: Enable the use of AI within confidential networks without the risk of data leakage.

---

6. Conclusion

The **National Network Security Framework (N²SF)** represents a shift from traditional network separation toward a more advanced model of governance. Its core elements include **role-based access control by data classification, protection of classified cloud environments, and AI-driven security controls**.

N²SF is not just a technical framework but also a cornerstone for achieving **organizational security governance**, ensuring that policies, operations, and governance structures align with evolving cybersecurity challenges. Future N²SF R&D will further strengthen this integration, enabling organizations to embed security as a governance principle across all operations.