REQUEST FOR COMMENT RESPONSE

Call for opinions on the "Draft Enforcement Order for the Act on Prevention of Damages Caused by Unauthorized Activities on Important Computers"

7 February 2026

I. INTRODUCTION

CrowdStrike appreciates the opportunity to provide our comments to the Cabinet Office of Japan on the Draft Enforcement Order for the Act on Prevention of Damages Caused by Unauthorized Activities on Important Computers (Draft Order).

CrowdStrike is an international cybersecurity company, based in the United States, that protects businesses around the world from globally-distributed cyber threats. We have extensive experience helping organizations prevent data breaches with a range of cybersecurity products and services including cyber threat intelligence; proactive hunting, incident response and managed security services; and an AI-powered software-as-a-service cybersecurity platform and marketplace.

II. COMMENTS

CrowdStrike commends the Government of Japan for its commitment to strengthening the cybersecurity posture of critical systems through the Act on Prevention of Damages Caused by Unauthorized Activities on Important Computers and this implementing enforcement order. As cyber threats continue to evolve in sophistication and scale, particularly against critical infrastructure and essential services, establishing clear frameworks for protection is essential.

We support Japan's risk-based approach to cybersecurity that focuses protective measures on systems deemed most critical to national security and public safety. This approach aligns with global best practices that prioritize the most consequential systems while avoiding unnecessary regulatory burden on less critical assets.

To strengthen the intent of the Draft Order and aid implementation we offer the following observations and recommendations:

A. Scope and Connectivity

The Draft Order currently defines “important electronic computers” to include computers that store important information and those “directly or indirectly” connected via telecommunications lines. This appropriately recognizes that protection must extend beyond

the computers storing important information to include connected systems that could serve as attack vectors. This network-based approach reflects the reality of modern attack techniques that often leverage trusted connections to reach high-value targets.

To keep the scope risk-based and prevent compliance effort from being diluted across low-impact systems we recommend that the order explicitly states that "indirectly connected" is intended to capture systems that can materially affect the confidentiality, integrity, or availability of the protected systems (e.g., administrative/control-plane systems, identity systems, management consoles, and other systems capable of materially impacting protected functions).

The Draft Order should explicitly end the scope of important electronic computers at the tenant/service boundary, and unrelated tenants and unrelated shared platform components should not be treated as automatically "in scope" by default. Regulated entities increasingly rely on managed security services that process telemetry in shared platforms (e.g., SIEM/MDR/threat hunting). To support adoption of these effective detection and response technologies while maintaining the law's intent we recommend that the scope explicitly excludes cloud, managed security services, and multi-tenant platforms.

B. Critical Infrastructure Focus

The inclusion of computers used by operators of social infrastructure, particularly those in Article 1(3) related to special social infrastructure operators, reflects an understanding of evolving threats to these sectors. We recommend ensuring that the definition remains flexible enough to accommodate rapid changes in technology and threat landscapes.

C. Classification Clarity

While the categories are well-defined, implementing organizations would benefit from additional guidance documents that provide specific technical criteria for determining whether systems fall within the scope. This would help ensure consistent application across different sectors.

D. Information Sharing Provisions

Public-Private Intelligence Sharing: Article 2 of the enforcement order designates specific organizations for information processing and analysis functions. The designation of NICT and JPCERT/CC as organizations that can receive and process cyber threat information represents a positive step toward formalized information sharing. We recommend establishing clear protocols and technical standards for such sharing to maximize effectiveness.

To support confident cooperation and sharing by regulated entities and their suppliers, we recommend developing governance safeguards for such sharing and processing covering purpose limitation, appropriate minimisation (preference for indicators/summaries where sufficient), retention limits, access control and auditability, and protection of confidential business information and third-party information (including other-tenant data in multi-tenant environments).

Once sharing mechanisms are in place, it could be useful to regulated entities for NICT and JPCERT/CC to encourage the development of sector-level threat baselines. These baselines can be informed by private sector intelligence sharing and commercial feeds, curated or facilitated by government bodies, and applied autonomously by regulated entities.

International Alignment: We encourage alignment of information sharing frameworks with international standards and mechanisms to facilitate cross-border collaboration against threats that are inherently global in nature.

Actionable Intelligence: To maximize the value of information sharing, we recommend focusing on mechanisms that produce actionable, timely, and contextualized intelligence that organizations can use to enhance their defensive posture.

Further Recommendations for Implementation

The Draft Order has the potential to materially uplift the security posture of important organisations in Japan and is a great opportunity to adopt modern and advanced approaches to cybersecurity. Based on our global experience helping organizations defend against sophisticated threats, we offer the following recommendations for effective implementation. These recommendations preserve the core objective or the order while improving clarity, operational feasibility, and consistency. They also support adoption of modern and advanced approaches to cybersecurity capabilities that can dramatically improve detection and response outcomes such as the EDR, SIEM, MDR, and threat hunting capabilities.

E. Implementation Guidance

We recommend national-level guidance (e.g., a central FAQ and an interpretation escalation mechanism) to provide practical steps for organizations to comply with the requirements, reduce inconsistent application across regions and sectors, and to support consistent procurement requirements.

As the effective date is set as 1 October 2026 and the overview anticipates promulgation in late March 2026, we recommend publishing such guidance and any subordinate rules that affect scope and operational expectations as early as feasible. Ideally this should be at least six months before the effective date to enable regulated entities and suppliers to update

architectures, contracts, incident procedures, and readiness activities in a controlled and effective way.

Implementation requirements should align with internationally recognized technical standards to promote interoperability and avoid conflicts for multinational organizations.

F. Avoid an unintentional requirement for domestic-only processing or storage of security telemetry/logs

Security monitoring and analysis depends on 24/7 operations and global threat correlation. To facilitate this many organisations process some security telemetry outside Japan, and SIEM log data may be stored outside Japan. We recommend that official guidance clearly confirm that overseas processing/storage is compatible with compliance when organisations apply appropriate technical and organisational safeguards (e.g., encryption in transit/at rest, robust access controls, auditing, tenant isolation, minimisation, and retention/deletion controls). This reduces inconsistent procurement interpretations and preserves strong security outcomes for Japan.

G. Threat-Informed Defense

In order to further enhance the effectiveness of measures to prevent and mitigate damage caused by unauthorized acts against important electronic computers, and to extend the usefulness of the intelligence sharing provisions in the Draft Order, we recommend that the Government encourage the adoption of threat-informed defense as a risk-based operational approach.

Threat-informed defense refers to an approach in which preventive, detective, and response measures are prioritised based on realistic adversary behaviour and threat scenarios relevant to the role, function, and sector of each organisation. By aligning security operations with credible threat activity, organisations can focus resources to defend against the attack techniques most likely to be used against them, and inform advanced cybersecurity techniques such as hypothesis-driven threat hunting to have an increased chance of identifying malicious activity. This materially improves early detection, response effectiveness, and overall resilience.

Rather than prescribing specific technologies or control implementations, non-binding guidance could encourage regulated entities to demonstrate how their security monitoring, detection, and response capabilities are aligned with relevant threat scenarios and adversary techniques. This would allow flexibility across sectors and organisational maturity levels, while maintaining consistency with the objectives of the Act.

In addition, encouraging a threat-informed approach would support more effective incident

readiness and improve the quality and timeliness of information sharing and analysis during cyber incidents, including cooperation with designated analysis bodies. Clear threat context can contribute to faster triage, more accurate impact assessment, and more efficient coordination during incident response.

As many cyber threats affecting Japanese organisations originate from transnational actors, threat-informed defense is strengthened by access to international threat intelligence and cross-border analytical perspectives. Recognising the role of global threat visibility in supporting domestic cybersecurity objectives would further enhance the practical effectiveness of the framework established under the Draft Order.

H. Capacity Building

The Government of Japan should invest in workforce development and organizational capability building to ensure that protected entities have the human resources and expertise needed to effectively implement modern and advanced security measures. Emphasis should be placed on training the workforce to be able to implement and operate modern and advanced approaches to cybersecurity.

III. CONCLUSION

CrowdStrike supports Japan's efforts to enhance the security of critical computer systems through this enforcement order. We believe that effective cybersecurity requires a risk-based, intelligence-driven approach that combines strong technical measures with organizational preparedness and international cooperation.

We encourage continued engagement with industry stakeholders throughout the implementation process to ensure that protective measures remain effective, practical, and aligned with the evolving threat landscape. To do this effectively, the Government of Japan should establish mechanisms for regular evaluation and updating of the enforcement order to keep pace with evolving threats and technologies. CrowdStrike remains committed to supporting these efforts through our threat intelligence, technology solutions, and cybersecurity expertise.

IV. CONTACT

We appreciate the opportunity to provide these comments and stand ready to provide any additional information or assistance that would be helpful in advancing our shared goal of protecting critical systems from cyber threats.

We would welcome the opportunity to discuss these matters in more detail. Public policy inquiries should be made to:

Drew Bagley

VP & Counsel, Privacy and Cyber Policy

Email: policy@crowdstrike.com

Brian Fletcher

Director, Public Policy APJ

V. ABOUT CROWDSTRIKE

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with one of the world's most advanced cloud-native platforms for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

Learn more: https://www.crowdstrike.com/.