UNCLASSIFIED

Communications Security Establishment
Centre de la sécurité des télécommunications

CCNSS CANADIAN COMMITTEE ON NATIONAL SECURITY SYSTEMS

BULLETIN

Edition 2 I June 2018

IN THIS EDITION

Security Assessment and Authorization

The security assessment and authorization (SA&A) process for National Security Systems is the mechanism by which risk to an IT system is understood, mitigated and consistently and measurably managed throughout its lifecycle.

Over the past 6 months, the CCNSS Secretariat, in conjunction with the nine CCNSS member departments, have been engaged in defining the SA&A Standard for the Security and Intelligence (S&I) Community.

The collaborative interdepartmental working group has taken the best practices from participating departments and emerging concepts from private industry, and have incorporated them into the draft CCNSS Standard. The next area of focus is implementation. Several tools are under development to expedite the various tasks within the SA&A process such as categorization, Threat Risk Assessment (TRA) development, security profile tailoring and assessment. Following testing, these tools will be incorporated in to the Standard to aid departments with efficient use of scarce IT Security resources across the GC.

During the CCNSS meeting on 14 May, the model for NSS authorization was discussed. As the culminating task of the system assessment process, authorization is key to risk acceptance, and ensures security is inherently built into NSS. To accurately understand and quantify the risk presented by the system while still in development, a series of interim authorization gates are included at various stages of completion to ensure that the CCNSS Committee may influence security decisions that will impact shared risk to the interconnected S&I Community.

Canada

RECENT APPROVALS

On May 14th, 2018, the Canadian Committee on National Security Systems (CCNSS) approved the *Standard on Emission Security (EMSEC),* and the *Security Classification Markings Standard.*

While these standards are effective immediately, it is understood that departmental implementation will take some time and considerable effort.

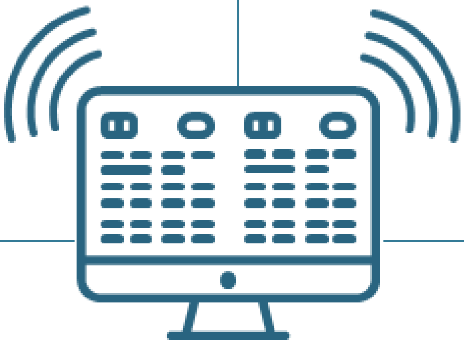
Please ensure that all stakeholders within your organization are made aware of these new standards and are consulted widely as you begin to plan your approach to come into compliance in the coming months.

Copies of these standards are available upon request from the Secretariat or on a self-serve basis from the CCNSS website on CTSN.

STANDARD ON EMISSION SECURITY (EMSEC)

Objective: to establish the criteria for consistent application of emission security measures in the protection of NSS.

DEFINITION	POLICY PRINCIPLES	COMPLIANCE	IMPLEMENTATION
Emission Security (EMSEC) is defined as a diverse program of measures, practices, application of safeguards and countermeasures that are designed to protect IT systems from information leakage due to Compromising Emanations (CE).	National Policy Principles for the application of Emission security are: • Emission security is proportional to need; • Physical access to potential areas of exploitation is denied; • Signals that encompass information are contained; and • Suppression of signals is done as close to the source as possible.	Compliance with this standard shall be achieved when NSS owners implement security controls prescribed in the standard that are appropriate to the NSS being protected.	Implementation ensures the security objectives of confidentiality, integrity and availability are being achieved as part of the overall risk management activities that are identified through a comprehensive Threat and Risk Assessment (TRA).



SECURITY CLASSIFICATION MARKINGS STANDARD

Objective: to establish a consistent practice of national security classification markings for information stored within or disseminated across NSS.

DEFINITION	POLICY STATEMENT	COMPLIANCE	IMPLEMENTATION
Security Classification Markings are markings which identify Sensitive Information used within a product, report, correspondence, message or similar material. Additional protection will be required for the information derived from or concerning sensitive sources, methods or techniques and only approved networks and similarly indoctrinated personnel may receive this material.	National Policy Principles for application of Security Classification Markings are: • Collaboration and information sharing is enabled through the consistent use of security control markings; • Security control markings enable incident response across the NSS; • Clear security control markings provide accurate means to label and store media and information; • Information properly categorized with appropriate security markings enable effective risk assessment of the NSS; • Access controls enforce logical access to information systems, information flow enforcement, separation of duties and principle of least privilege; and • Security labels (security attributes) provide access control based on information classification and caveat.	Compliance with this standard shall be achieved when NSS owners implement security control markings as prescribed in the standard for the NSS being protected.	Implementation ensures the proper marking of sensitive documents and enables the proper control and access to information based upon need-to-know principles and access to the NSS involved.

RECENT DISCUSSIONS

Physical Security

Physical security is a countermeasure put in place to deter and eliminate unauthorized physical access to a given location. Access to information assets are further limited to those with need-to-know authorization.

The enforcement of physical security safeguards enables organizations to lower risks, and the importance of physical security within National Security environments is crucial to protecting Canadians, partners, and other stakeholders.

Canadian NSS are systems through which national security activities are enabled and protected. NSS information, resources and assets are of such sensitivity that if compromised, could undermine the national security of Canada and its partners.

The CCNSS recently authorized its Secretariat to strike an interdepartmental working group with PSPC, RCMP, TBS and other key stakeholders to collaborate on much-needed updates to the existing National Physical Security Standard to address several gaps with regards to National Security environments.

The inventory of National Security Systems exceeds three hundred systems, located both domestically and abroad, often in multi-tenant facilities alongside other systems. Since the information held in those systems may originate under different intelligence authorities, a more holistic approach to physical security is needed to clarify jurisdictional issues and applicability of policies and standards in these complex National Security environments.

FUTURE MEETING AGENDAS

SEMPTEMBER 2018	
Approval of Standards	• Access Control Management Standard • Security Assessment and Authorization Standard
Approval of Principles	• Physical Security Standard
Discussion	• Compliance Regime for NSS • Incident Management Process for NSS • NSS Threat Assessment Management
DECEMBER 2018	
Approval of Standards	• Physical Security Standard
Approval of Principles	• Compliance Regime for NSS • Incident Management Process for NSS • NSS Threat Assessment Management
Discussion	• Access Attribute Management

CONTACT US

CCNSS Secretariat staff can be contacted at:

✉ CCNSS-Secretariat-mdl@ctsn-rcts.gc.ca

✉ CCNSS-Secretariat@cse-cst.gc.ca