Communications Security Establishment | Centre de la sécurité des télécommunications

CCNSS CANADIAN COMMITTEE ON NATIONAL SECURITY SYSTEMS BULLETIN

Edition 1 I March 2018

IN THIS EDITION

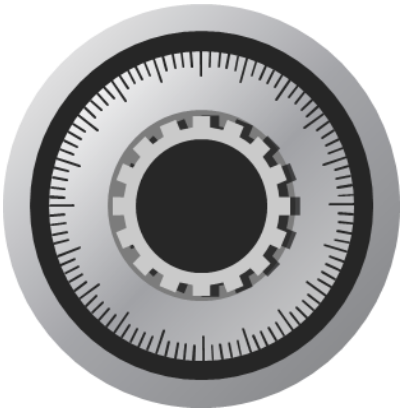
RECENT APPROVAL OF TWO NEW STANDARDS

RECENT DISCUSSION ON CEO MATERIAL

FUTURE MEETING AGENDAS MAY AND SEPTEMBER

CONTACT US

What is CCNSS?



The Canadian Committee on National Security Systems (CCNSS) was established by Deputy Ministers of National Security to govern Government of Canada (GC) National Security Systems (NSS) through the development of national standards and enterprise approaches that promote the consistent application of security.

The CCNSS's main responsibility is to oversee the protection of NSS, while enabling secure interoperability within the Canadian Security and Intelligence community, as well as with Allied organizations, today and into the future.

A Canadian NSS is a system within which national security activities are enabled and protected. Information, resources and assets are of such sensitivity that compromise could undermine the national security of Canada or its partners. The security measures required for a NSS are designed to provide confidence and defence against the most sophisticated threat.

The CCNSS is chaired by the Deputy Chief of Information Technology Security (CSE) and consists of a Committee, a Secretariat, and various Working Groups. Members, participants of the committee, the secretariat and the working groups, and Subject Matter Experts are drawn from Member departments. The CCNSS meets quarterly, and on an ad hoc basis as required.

Committee membership includes Assistant Deputy Ministers from CSE, the Department of National Defence, the Privy Council Office, the Royal Canadian Mounted Police, the Canadian Security Intelligence Service, Public Safety Canada, Shared Services Canada, Treasury Board Secretariat, and Global Affairs Canada. CSE provides the executive secretariat function, which supports the CCNSS.

RECENT APPROVALS

On 11 December 2017, the Canadian Committee on National Security Systems (CCNSS) approved the *Standard on Security Controls for Protection of NSS*, and *the Standard for the Sharing of Information via Collaboration Tools on National Security Systems*.

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 SECURITY CONTROLS FOR PROTECTION OF NATIONAL SECURITY SYSTEMS

Objective: to establish the criteria for consistent application of security controls that will be used for the protection of all applicable NSS prior to authorization.

DEFINITION	POLICY PRINCIPLES	COMPLIANCE	IMPLEMENTATION
Security Controls are defined as a set of *protection measures* that are designed to support the business activities of the NSS owners and ensure *trust* and *confidence* in the protection of the information assets and business functions being performed	National Policy Principles for application of security controls across the NSS spectrum are: • Controls derive from approved national guidance and authoritative sources and best practices; • Controls align with partners and enable sharing of information; • Controls are proportionate to sensitivity of information and risk; and • Incident reporting aids situational awareness and management of security threats, vulnerabilities, risk assessment, and for the management of security controls.	Compliance with this standard shall be achieved when NSS owners implement security controls prescribed in the profile appropriate to the NSS being authorized as follows: • Security controls will be established based on three profiles: **Baseline** (all NSS), **Classified** (any NSS holding classified info up to TS with no caveats), and **Compartmented** (with caveats); and • Each profile is complementary and cumulative, so subordinate profiles must also be implemented.	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).

STANDARD FOR THE SHARING OF INFORMATION VIA COLLABORATION TOOLS ON NATIONAL SECURITY SYSTEMS

Objective: to state principles by which to govern sensitive information sharing on NSS, and to define minimum policy requirements for Departments to address via policy or procedures.

DEFINITION	POLICY STATEMENT	COMPLIANCE	IMPLEMENTATION
Collaboration Tools are defined as any system or network application where users can share information with others (includes email and web collaboration environments).	Deputy Heads are responsible for ensuring that all sharing of information carried out by users within their departments is in accordance with the following principles: • The sharing of information complies with all relevant legislative and national policy instruments, including each department's enabling legislation; and • Sensitive information is handled in a manner that reduces the risk of compromise of the information and corresponding sources of information.	Compliance with this standard shall be achieved when Departmental Procedures are implemented that respect the Principles in the Policy Statement and address: • Designation of a departmental NSS Collaboration Authority; • Ensuring the lawful sharing of information; • Information management requirements; • Protection of sensitive information; and • Ensuring compliance.	Implementation begins with the establishment of a Departmental NSS Collaboration Authority, who: • Ensures departmental procedures are in place prior to approving collaboration tools on NSS; • Approves the use of collaboration tools on NSS; • Establishes an approval process for user access to collaboration tools; and • Ensures users are clear on what information can be shared, with whom, and conditions for sharing including handling and prescribes retention requirements, ATIP responsibilities and oversight bodies' access.

RECENT DISCUSSIONS

Updated guidance on the access to CEO Material

The CCNSS also recently reviewed how the Canadian Eyes Only (CEO) dissemination control term has been used and its effects on the distribution of information to Canadians and Foreign Integrees employed within the Government of Canada (GC). In the past, a few departments have shared CEO material with Foreign Integrees, who are treated as domestic personnel while employed in Canada, by having them sign Non-Disclosure Agreements (NDA).

As more GC departments become increasingly integrated, it becomes more difficult to maintain consistent restrictions on CEO material. This increased connectivity poses new security risks for CEO content, even if it is being shared with Foreign Integrees with the best intentions.

The CCNSS requests that organizations review their use of NDAs for Foreign Integree access to national information, and restrict CEO material access to Canadians only, by no later than 31 December 2019.

This new direction on CEO will be reflected in the new *Standard on Security Control Markings for National Security Systems*, to be released in FY 2018/2019.

The CCNSS Secretariat is available for consultation should Departments wish to discuss the specific impacts to their organizations, and to assist with determining an appropriate implementation schedule.

FUTURE MEETING AGENDAS

MAY 2018	
Discussion	• Physical Security • Security Assessment and Authorization Standard (Decision)
Approval of Standards	• EMSEC Standard • Security Control Marking Standard
Approval of Principles	• ABAC/IDAM Standard
SEPTEMBER 2018	
Discussion	• Incident Management Standard • Threat Assessment Management • Risk Management Framework
Approval of Standards	• ABAC/IDAM Standard • Security Assessment and Authorization Standard
Approval of Principles	• Physical Security

CONTACT US

CCNSS Secretariat staff can be contacted at:

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

CCNSS-Secretariat@cse-cst.gc.ca