Guidelines on Threat and Risk Assessments

1. Effective Date

These guidelines are effective as of April 1, 2017.

The guidelines will be reviewed as needed or at a minimum every five years by the Departmental Security Officer (DSO) in consultation with Regional Security Offices (RSO).

2. Application

These guidelines apply to:

a. Security practitioners responsible for the conduct of threat and risk assessments (TRA) on departmental occupied premises; and

b. Site managers, responsible for the proper safeguarding and destruction of protected/classified information (paper and electronic) and assets, and for ensuring that the security requirements of the site, based on the TRA and its recommendations, are implemented, maintained and monitored accordingly.

c. Employees

3. Context

The nature of the Department's mandate dictates the way that departmental business and client information should be collected, stored and handled. Canadians entrust ESDC with the management of their personal information and all other information (related to finances, passports, processes, etc.) that requires robust privacy and security controls and processes.

ESDC is responsible for ensuring the safeguarding of employees and visitors in all locations including those who occupy space with other organizations; and the security of departmental premises, information and valuable assets.

Initial TRAs are required to be conducted for every ESDC occupied site, including telework arrangements and support locations as required (off-site

facilities, e.g. business continuity planning back-up sites) to ensure that departmental premises, operations, information, systems/networks and other departmental assets are properly safeguarded accordingly.

TRAs are to be revised every five (5) years from the last site review date or sooner when there are circumstances that could result in a changed threat environment as outlined below.

The revision and update of an existing TRA or completion of a new TRA is required within one (1) year whenever there are any of the following changes to a departmental occupied site or support location:

- Change in physical configuration (building upgrades etc.)
- Change in floor layout (i.e. Workplace 2.0, new secured zones, public access zones etc.)
- A significant change in occupancy numbers
- Significant increase in sensitive information or valuable assets
- Changes in site access, entrance points or emergency exits
- Modification of security systems (access control, alarms, gates, guard services etc.)
- Change in external environment (significant changes in landscaping, new co-location or neighbouring organization, increased external threats)
- Significant security incident(s) occurrence (ie: break in)
- When the type of business offering changes or there are additions made to service offerings.

4. Acronyms/Definitions

DSO	Departmental Security Officer
ISB	Integrity Services Branch
Site Manager	An employee of the Department who occupies a position of authority and who is responsible for the site and its operations (e.g. Director, Manager, or other delegated official)
Site Reviews	Site reviews consist of a visual / physical security inspection of the worksite. The reviews also assist with the identification of existing security measures, a history of new or existing incidents and the opportunity to enhance security based on new threat environments. These could be onsite TRAs or virtual TRAs depending on the circumstances.
RSO	Regional Security Office
Staff	Employees (indeterminate and term), students, casuals
Other Individuals	Contractors and/or consultants
Visitors	Individuals that have impeded access to the department such as: public, partners, family members, and employees from other Government Departments

TRA	Threat and Risk Assessment – a process that involves the physical review of a site on security measures for the protection of departmental premises, employees, information and other valuable assets entrusted to the department.

5. Legal Consideration Statement

During the conduct of TRAs, consideration must be taken to ensure that security measures do not impede or impact on acts and legislations pertaining to life safety and privacy requirements (e.g. *National Building Code of Canada, Canada Labour Code, National Fire Code of Canada and related codes and standards, Privacy Act*).

6. Objective and Expected Results

6.1 Objective

The objective of these guidelines is to set out processes and protocols to be adhered to by security practitioners, in collaboration with the Departmental Security Officer (DSO) in the conduct and management of TRAs for all ESDC occupied and support space.

6.2 Expected Results

The expected results of these guidelines are to:

- Develop consistency in process, protocols and timelines for TRAs within the Regional Security Offices (RSO);
- Clarify the roles and responsibilities associated with TRAs;
- Monitor the protocols and progress to ensure compliance; and
- Provide an official avenue to report to the DSO on the state of security within ESDC.

7. Roles and Responsibilities

Departmental Security Officer (DSO)

7.1 The Departmental Security Officer (DSO) is responsible for the following:

- Leading the development and maintenance of a departmental security plan that:

        - Provides an integrated view of departmental security risks and requirements, including considerations for external stakeholders; and
        - Defines strategies, priorities, responsibilities and timelines for strengthening and monitoring departmental security management practices and controls;
    - Advising the deputy head and other stakeholders on security management matters;
    - Overseeing the establishment of TRAs and related processes and reporting on the status of TRAs and related recommendations to the deputy head and other stakeholders;
    - Ensure a consistent departmental approach, the identification and analysis of trends, and sharing of best practices and innovative approaches in the conduct of TRAs;
    - Overseeing the establishment of department-wide processes for assessing and documenting actions taken regarding residual security risks for the department's programs and services and their supporting resources, including ongoing analysis to continually improve security practices; and
    - Overseeing the establishment of department-wide processes to monitor and ensure a coordinated response to and reporting of department-specific threats, risks, vulnerabilities and security incidents, and, where required, implementing any recommended changes.

Regional Security Offices (RSOs)

7.2 The Regional Security Office (RSO) is responsible for the following:

- Conducting TRAs in collaboration with site managers, on all ESDC occupied and back up sites to counteract assessed threats to human life, premises, operations, information and other valuable assets. This would also include any Memorandum of Understanding (MOU)/agreement with other departments, agencies, other levels of government or private sector organizations;
- Conducting a TRA every five (5) years from the last site review date or sooner when there are circumstances that could result in a changed threat environment as outlined in Section 3;
- The determination of a TRA will be based on the premise that:
    - The review of the site identifies existing physical security measures/systems;
    - Related policies, standards and directives are adhered to;
    - Threats and vulnerabilities to the site are identified;
    - Recommendations are made to enhance any existing security measures and/or systems deemed deficient; and

    - An evaluation is provided on cost-effective options for upgrades as required.
- Ensuring that every ESDC site within the respective region has undergone a TRA and report on the status of TRAs and related recommendations via the centralized database;
- Ensuring that the TRA report is released in a timely manner to the appropriate stakeholders for action/implementation of recommended safeguards and follow-up on implementation status;
- Ensuring that an original copy of the TRA is kept in the region for reference as required;
- Ensuring that priority levels (High, Medium, Low) are established for each TRA recommendation based on risk;
- Monitoring and maintaining communications with the responsible site management on the status of TRA recommendations made and following up on any outstanding items requiring immediate corrective action; and
- Sharing best practices or innovative approaches as applicable in the conduct of TRAs.

Managers

7.3 Managers at all levels are responsible for the following:

- Informing the RSO of any issues regarding policy compliance, changes in individual behaviour or operations that may be cause for security concern, or security incidents within their area of responsibility;
- Cooperating with the RSO in the TRA process/site review and assisting in identifying and implementing corrective remedial actions;
- Integrating and applying safeguards from TRAs as directed by site management and RSOs; and
- Report to the RSO the status of implementation on the required safeguards and recommendations of TRAs.

Employees

7.4 All employees are responsible for the following:

- Safeguarding information and assets under their control, whether working on-site or off-site, or while travelling in accordance with departmental security practices;
- Raising any security concerns with their managers and/or RSO when identified; and
- Cooperating with the RSO when asked, to address any concerns that may impact on security and/or personal safeguards.

8. References

This Directive should be read in conjunction with or in reference to:

8.1 Legislation

- ***Privacy Act***
- D***epartment of Employment and Social Development Act (DESDA)***

8.2 Treasury Board Secretariat (TBS) Policies, Directives and Standards

- ***Policy on Government Security (PGS)***
- ***Operational Security Standard on Physical Security(to be updated once the revised PGS in is effect)***
- ***Operational Security Standard: Management of Information Technology Security (MITS)(to be updated once the revised PGS in is effect)***

8.3 ESDC Corporate Policy Instruments

- ***Departmental Security***
- ***Physical Security***
- ***Threat and Risk Assessment Checklist***
- ***Clean Desk Guidelines***
- ***Information Classification Guide / Appendix 3***
- ***ESDC Storage of Electronic Information Directive***
- ***ESDC Code of Conduct***

9. Enquiries

Questions concerning this directive can be addressed by the Regional Security Office. **(http://iservice.prv/eng/is/security/contact_us/rso_contacts.shtml**