Annex A

Statement of Requirement

Data Centre Co-location Services

1 Introduction

Shared Services Canada (SSC), hereafter referred to as “the Client”, has a requirement as detailed herein to acquire high availability, existing commercial data centre co-location services to be delivered by a Contractor from one single location within a range of not less than 10 kilometres in straight line distance from Angus Ontario (Latitude, Longitude: (44.313872, -79.8842912)), and not more than 100 kilometres of installed fibre network distance as measured from Angus Ontario (Latitude, Longitude: (44.313872, -79.8842912)).

A co-location service is defined as a service provisioned from a controlled and managed data centre space, where multiple customers locate and administer their own network, server and storage equipment and interconnect to a variety of telecommunications and other network service provider(s) with a minimum of cost and complexity.

The requirement to acquire existing secure highly reliable data centre capacity through the use of this co-location service will be:

a) based on industry accepted standards and criteria, with environmentally responsible design and operation, and delivers continuous, uninterrupted data centre support for IT processing as described herein;

b) physically located to enable high availability fail over of IT processing subsystems between primary data centres and the co-location service, through use of telecommunications protocols as described herein;

c) configured to accommodate a range of IT power requirements from 250 Kilo-Volt Amperes (kVA) up to 2,000 kVA, and a range of cabinet power densities from 5 to 20 kVA, and stand alone IT equipment densities of up to 150 VA per square foot, as described herein;

The Contractor must meet the following implementation timeframes:

a) The Client Fit-up Date is defined as the date the Contractor’s co-location service is deemed to have successfully completed the Client Data Hall Acceptance Testing Procedure (Section 4.4.4 herein) and is no more than 70 calendar days after contract award. The Client Fit-up Date is the beginning of the client activities required to configure the co-location service ready to accept Client workloads.

b) The Client In-Service Date is 100 calendar days after contract award and is defined as the date that the Contractor will commence billing the Client for the co-location base service.

All services described herein are considered inclusive and covered as part of the base services cost specified in Annex B, Pricing Tables. For any services not included in the base services cost line item, the Contractor must provide those services in accordance with the prices set out in Annex B**.**

2 Technical Requirements

2.1 Contractor Facility

2.1.1 Availability

a) The Contractor must provide a co-location service that meets the operational requirements described in this document and is accessible to the Client on a 24 hours a day, 7 days a week, 365 days a year (366 days in leap years) basis (hereinafter referred to as "at all times") necessary to meet 100% availability throughout the Contract period.

2.1.2 Maintenance

a) The Contractor must ensure that the Contractor Facility is well maintained such that it can meet its designed availability level at all times throughout the Contract period. This maintenance must include at a minimum, but is not limited to:

i) Removal of ice and snow from all outside parking spaces and the roadways, walks, steps and fire escapes leading to and from the premises;

ii) Cleaning of all common areas such that they are kept tidy, free and clear of any refuse, garbage, waste products and obstructing materials;

iii) Removal of garbage from the premises whenever and so often as may be necessary, not less than once daily;

iv) Cleaning and repairs required to keep wash room equipment and accessories in good operating condition;

v) Ground maintenance and window cleaning; and

vi) Repair and upkeep of HVAC systems, Life and Safety Systems and elevators (as applicable).

2.1.3 Loading Docks

a) The Contractor must provide Client access to a loading dock and receiving area at the Contractor Facility at all times.

d) The Contractor must provide mechanical lifting device(s) to move the Client IT equipment from the receiving area to the Temporary Secure Storage Area (defined herein) and/or the Client Data Hall (defined herein).

2.1.4 Storage and Disposal

a) The Contractor must provide a minimum of 40 square metres of temporary storage (hereinafter referred to as the "Temporary Secure Storage Area") for the Client's IT infrastructure. The Temporary Secure Storage Area is managed, controlled and accessible by the Contractor only and is available to the Client at all times.

b) When a Client representative is on-site or present at the Contractor Facility loading dock, to receive IT equipment and/or other related government property, the Contractor will have a procedure and system in place at all times to complete the following requirements:

i) The Contractor will log the receipt of goods from the Client. Under no circumstances will the Contractor be accepting these goods on behalf of the Client this will be the sole responsibility of the Client Technical Authority.

ii) The Contractor will move the Client equipment to the Temporary Secure Storage Area or Client Data Hall defined herein, as directed by the Client representative.

e) If no Client representative is on-site or present at the Contractor Facility loading dock, to receive IT equipment and/or other related government property , the Contractor will have a procedure and system in place at all times to complete the following requirements:

iii) The Contractor will log the receipt of goods from the suppliers on behalf of the Client.

iv) The Contractor will move the Client equipment to the Temporary Secure Storage Area.

f) When requested by the Client, the Contractor will move the Client equipment from the Temporary Secure Storage Area to the Client Data Hall.

g) When requested by the Client, the Contractor must un-crate the Client equipment in a support area specifically dedicated for this task and dispose of crate and packing materials in a manner that is environmentally responsible (e.g. recycle).

h) Un-crating of equipment is not permitted in the computer room and/or Client Data Hall at any time.

i) The Contractor must provide a minimum of 6 square metres of secure locker area separate from the Client Data Hall that is accessible only to the Client.

2.1.5 Co-location Common Areas

a) The Contractor must provide Client access to common areas within the Contractor Facility at all times, such as but not limited to:

i) Washrooms;

ii) Lunch Room;

iii) First Aid Room;

iv) Meeting Room; and

v) Office Cubicles;

j) When requested by the Client, the Contractor must provide access to an onsite furnished meeting room to accommodate a minimum of 10 people, with active and ready-to-use power receptacles, active and ready-to-use teleconferencing, active and ready-to-use projector and screen, and active and ready-to-use high-speed internet access capabilities at all times.

k) The Contractor must provide a minimum of 2 furnished office cubicles as follows:

i) That is shared among all Contractor customers and available to the Client on an on-demand basis, with 24 hours notice to the Contractor.

ii) The office cubicles must be provided in a separate closed office space or room within the facility that prohibits access except through electronically controlled access points to authorized persons.

iii) each cubicle must have access to :

1) active and ready-to-use high-speed Internet; and
2) active and ready-to-use landline connected telephone;

2.1.6 Power and Cooling Systems

a) The Contractor must provide the availability of the Power and Cooling Systems 100% of the time. Shutdowns of the power and cooling systems that affect computer room operations for equipment maintenance or replacement are not permitted.

b) The Contractor's co-location service must incorporate the Uptime Institute's Tier III performance objective or its equivalent, see Appendix H. The Uptime Tier III objectives defined herein do not inherently eliminate single points of failure. As such, the Contractor must implement safe guards against any single points of failure in the mechanical and electrical systems.

c) The contractor's cooling design must have the capability of providing cooled liquid to the IT cabinet level in support of future generation, high density, computing platforms. The future implementation of this design must not impact service to the Client.

d) The Contractor must provide on-site generator power that supports uninterrupted, continuous operation of the Co-location Service during all periods when power is unavailable from the power company. The engine-generator must not have runtime limitations. Standby engine generators do not qualify. Additionally, the engine generator plant must be concurrently maintainable while carrying the critical load.

b) The Contractor must employ emergency power generators that meet or exceed all requirements for Tier II emissions and standards.

English

http://www.ec.gc.ca/CEPARegistry/regulations/detailReg.cfm?intReg=88

French
http://www.ec.gc.ca/registrelcpe/regulations/detailReg.cfm?intReg=88

c) The Contractor must configure the Co-location Service to accommodate initial peak power requirements, plus 10 percent.

d) The Contractor must configure the Co-location Service to include a dual active-active conditioned power bus configuration to all Client cabinets and standalone IT equipment, regardless of circuit type and receptacle requirements.

e) The Contractor must supply dedicated, standalone, data centre class, Power Distribution Units (PDU) that deliver the Client Data Hall power requirements.

f) The Contractor must supply, throughout the Contract Period, dual electrical power and environmental conditioning to the entire Client's IT equipment during maintenance activities.

g) The Contractor must provide IT electrical grounding systems in accordance to current standard TIA-942.

l) The Contractor must provide emergency power to all common areas (defined herein) at all times.

2.1.7 Facility Telecommunications Rooms

a) The Contractor must , for the Contract Period, grant the Client's telecommunications providers, access to the facility telecommunications rooms to allow such providers:

i) To install, maintain, operate, repair, replace, and remove communications equipment required to provide the Client with network connectivity, on and in the Telecommunications Rooms (as described in 2.2.2 Network Requirements) on the lands and buildings used by the Contractor for the supply of Co-location Services (the "Property");

ii) To install, maintain, operate, repair and replace certain connecting equipment (the cables, conduits, inner ducts, connecting hardware and other passive equipment together with the right to pull that connecting equipment through the Property's "Entrance Link" (defined as the core sleeve penetration through the Property foundation) and through other "Property Communications Spaces" defined as the telecommunications pathways necessary to reach from the Entrance Link to the Telecommunications Rooms, as may be necessary to provide telecommunications services to the Client.

iii) the right of ingress and egress for the Telecommunications employees, servants and agents and the use of the elevators, entrances lobbies, hallways, stairways, driveways and common loading areas in and about the Property.

2.1.8 Security

a) The Client Data Hall (defined herein) must be a Security Zone, (an area to which access is limited to Client authorized personnel). Security screening requirements as specified in the contract will apply to the Security Zone. Details for security zoning are found at:

English

http://www.rcmp-grc.gc.ca/physec-secmat/pubs/g1-026-eng.htm

French

http://www.rcmp-grc.gc.ca/physec-secmat/pubs/g1-026-fra.htm

b) The Security Zone (as defined in 2.1.8 a.) must be accessible only from an Operations Zone, (an area to which access is limited to personnel who are authorized to work in this area). The Security Zone perimeter must have slab to slab walls that meet the specifications found in:

Appendix I – Document "G13-01 Secure Storage Rooms";
Appendix I – Document "G13-02 Secure Demising Wall".

c) The Security Zone must be constructed to include Radio Frequency Shielding as detailed in the Communications Security Establishment Canada (CSEC) document ITSG-02 found at:

English

http://www.cse-cst.gc.ca/its-sti/publications/itsg-csti/itsg02-eng.html

French

http://www.cse-cst.gc.ca/its-sti/publications/itsg-csti/itsg02-fra.html

d) The Contractor agrees that all who require access to the Operations Zone must be cleared to a minimum of Reliability Status by the PWGSC CISD organization at no cost to the Client. It is the Contractor's responsibility to establish a process and to negotiate a cost with the PWGSC CISD to perform this service. CISD reference material can be found at:

English

http://ssi-iss.tpsgc-pwgsc.gc.ca/ssi-iss/personnel/enqut-scrnng-eng.html

French

http://ssi-iss.tpsgc-pwgsc.gc.ca/ssi-iss/personnel/enqut-scrnng-fra.html

If the Contractor has customers that occupy an area of the Co-location facility that do not meet the screening requirements of 2.1.8 d., then the Contractor must separate this area from the Operations Zone and Security Zone, as applicable, by a penetration resistant wall that meets the specifications of section 2.1.8 b.

e) The Contractor must not impose any changes to the Client as a result of an existing customer obtaining a higher security profile, such as Top Secret.

f) The Contractor Facility must have continuous video surveillance and alarm monitoring at all times for the areas including but not limited to all entrances to the property and Contractor Facility, entrances to the Client Data Hall, security zone, operation zone, loading docks, parking areas, roof and all areas immediately within the perimeter of the property.

g) The Contractor must record and store the surveillance video for no less than 180 calendar days, and be available for review by the Client's Security Authority on a when requested basis. If requested, the video must be provided to the Client within 24 hours from the time the request is made.

h) The Contractor must provide the capability for the Client to interconnect with the Contractor's real-time video surveillance system for video monitoring specific to the Client Data Hall.

i) The Contractor must protect the Client IT equipment through use of multi-zone fire monitoring, detection and suppression systems. Fire suppression must be provided at a minimum by a double pre-action interlock sprinkler system.

2.2 Co-location Requirements

2.2.1 Client Data Hall Requirements

a) The term "Client Data Hall" refers to the area of the contractor's data centre dedicated to the Client's information technology infrastructure. The Client Data Hall shall include the Client's primary area and all the Client's secondary areas that may be included, unless explicitly referenced separately.

b) The Contractor must design and provide the Client Data Hall to meet the following requirements:

   i) configuration changes must be conducted in a manner that does not interrupt the Data Centre Co-location Service (DCCS) to the Client;

   ii) if the primary space allocation cannot be expanded, the Contractor will expand or provide a secondary space to the Client, in which the Client network can to be interconnected with the primary space without any network security vulnerabilities to the Client. All physical security requirements for the primary area will apply to all secondary space;

   iii) access points must be electronically controlled;

   iv) data halls must be protected from unauthorized access through the ceiling or under the floor; and

   v) physical control must extend to the network cabling coming into the primary space through the provision of rigid conduit and armoured cable;

c) The Contractor's facility must accommodate Client Data Hall floor loading associated with fully populated cabinets weighing up to 1,000 kilograms.

d) The Contractor must install and provide active and ready-to-use dual electrical power from the Contractor's power distribution units to the Client cabinets and standalone IT equipment located in the Client Data Hall.

e) The Contractor must provide active and ready-to-use convenience electrical outlets for maintenance personnel in accordance with local building codes within the Client Data Hall.

f) The Contractor must provide 2 active and ready-to-use landline telephone jacks within the primary Client Data Hall and each of the secondary Client Data Halls.

g) The Contractor is not authorized to enter the Client Data Hall without prior written consent from the Technical Authority, with the exception of responding to an emergency situation, such as a fire. In such event(s), Contractor's access must be reported to the Client in accordance with the incident management reporting requirements as described herein.

h) The Contractor is not authorized to move any Client computing assets from the Client Data Hall without prior written consent from the Technical Authority.

i) The Contractor may request in writing to the Technical Authority that a data hall be moved to another location within the Contractor Facility. It will be at the sole discretion of the Technical Authority to either reject or accept the change request, subject to the following minimum condition:

   i) the Contractor will solely be responsible for all costs associated with the move of the data hall including but not limited to, the Contractor's costs; the Client capital costs, the Client one-time costs; and the Client operational costs;

j) The Contractor must allow the Client to arrange for the cleaning inside Client IT cabinets at the Client expense.

k) The Contractor must provide under-floor cleaning services for all raised floor areas, and floor cleaning for all on-slab floor areas, at a minimum once per year in accordance to the ISO 14644-1 Class 8. This standard can be found at:

   English

http://www.iso.org/iso/home.html

French

http://www.iso.org/iso/fr/home.htm

The Contractor must notify the Technical Authority in writing a minimum of 90 calendar days in advance of the scheduled cleaning.

2.2.2 Network Requirements

a) At a minimum, the Contractor must include the following connectivity requirements at the Contractor Facility:

   i) provision of dual distinct and separate underground conduits for network cabling from the contractor's property line to the Contractor Facility network entry points (Entrance Links) that are separated by a minimum of 10 metres from each other to mitigate risk of damage or failure; as necessary to achieve 100% in-service availability at all times; and must provide ready-to-use carrier neutral multiple diverse high speed network paths for multiple telecommunication service providers that service the Contractor's facility area, at the contractor's cost;

   ii) provide two separate telecommunications rooms with maximum feasible separation, but no less than 10 metres, to achieve 100% in-service availability at all times, each equipped with a secure network path to a separate contractor facility network entry point (Entrance Link) to accommodate and to include ready-to-use points of presence as required for the carrier neutral telecommunications service providers at the contractor's cost;

   iii) provide secure network cabling paths from each of the telecommunications rooms to the Client Data Hall to accommodate and to include ready-to-use points of presence as required for the multiple telecommunications service providers at the contractor's cost;

   iv) The contractor must provide a cable management system for network interconnectivity within the Client Data Hall. The Client is responsible for the cable plant architecture and design; and

b) The Contractor must secure the common telecommunications rooms and allow controlled access to authorized contractor and telecommunications service provider personnel only.

2.2.3 Power Requirements

a) The Contractor must provide the following "baseline reserve power", notwithstanding incremental growth requirements, as of the Client Fit-up Date as follows:

   i) 250 kVA; consisting of 90% cabinet mount equipment and 10% standalone equipment.

b) The Contractor must provide the Client Data Hall with the electrical infrastructure to support a range of cabinet power densities from 5 to 20 kVA and stand alone equipment requiring 3 phase 208V, with densities of up to 150 VA per square foot, as of the Client Fit-up Date.

c) The baseline reserve power identified in 2.2.3 a) will be the baseline reserve power for the Contract Period.

3 Operational Support Requirements

3.1 Service Support

3.1.1 Service Desk

a) The Contractor must provide a Service Desk as a central point of contact and record for all incidents, problems, service requests, change requests, general assistance and information requests related to the Co-location Service.

b) The Contractor must provide a detailed description of its Service Desk organization and processes to the Technical Authority no less than 40 calendar days after the contract award date.

c) The Contractor must provide the Client with a local telephone number and/or toll free number for access to the Service Desk no less than 40 calendar days after the contract award date.

d) The Contractor's Service Desk must be available at all times

e) The Contractor must provide service in both official languages, English and French, at all times.

3.1.2 Incident Management

a) The Contractor must provide the detailed Incident Management processes to the Technical Authority no less than 40 calendar days after the contract award date to meet the minimum requirements of:

   i) Schedule A: Response Targets for Incident Management.

   ii) Schedule B: Response Targets for Security Incident Management

b) The Contractor must provide priority response to the Client for incidents based on their impact on service availability as described in:

   i) Schedule A: Response Targets for Incident Management.

   ii) Schedule B: Response Targets for Security Incident Management

c) The Client will escalate when incidents are not addressed in accordance with:

   i) Schedule A: Response Targets for Incident Management.

   ii) Schedule B: Response Targets for Security Incident Management

d) The Contractor must provide a secure Internet-based service for the Client to, at a minimum:

   i) Open Incident Records to capture the following information:

      1) Description of Incident ;

      2) Impact to Client; and

      3) Priority

   ii) Monitor the status of active Incidents, including:

      1) Status of Contractor Activities; and

2) Status of Possible Delays to close the incident

iii) Review completed and/or cancelled Incident Resolution Requests, for the past 12 consecutive months.

e) The Contractor must provide accounts for the Incident Resolution Request Web service to all personnel identified by the Technical Authority per Schedule C: Response Targets for Change Management.

3.1.3 Problem Management

a) The Contractor must provide a detailed Problem Management processes to the Technical Authority no less than 40 calendar days after the contract award date which must include the following activities:

i) Lifecycle management of all problems

ii) Determine the root cause of incidents

iii) Ensure that the resolution of the problems have been implemented through the change control process

iv) Trend analysis of incidents

b) The Contractor must provide a secure Internet-based service to allow the Client to, at a minimum:

i) Make Problem Resolution Requests to capture the following information:

1) Description of Request;

2) Requested Resolution Date;

3) Impact to Client; and

4) Priority

ii) Monitor the status of active Problem Resolution Requests, including:

1) Status of Contractor Activities; and

2) Status of Possible Delays to remedy problem

iii) Review completed and/or cancelled Problem Resolution Requests, for the past 36 consecutive months.

c) The Contractor must provide accounts for the Problem Resolution Request Web service to all personnel identified by the Technical Authority per Schedule C: Response Targets for Change Management.

3.1.4 Change Management

a) The Contractor must provide a detailed Change Management processes to the Technical Authority no less than 40 calendar days after the contract award date as specified in the contract that meets the requirements stated in Schedule C: Response Targets for Change Management.

b) The Contractor must provide a secure Internet-based service to allow Clients to, at a minimum:

i) Make Change Requests to capture the following information:

1) Description of Request;

2) Requested Change Date;

3) Priority;

4) Use of Optional Services; and

5) Special instructions, such as but not limited to, the planning, coordination and installation of large IT equipment in the Client Data Hall.

ii) Monitor the status of active Change Requests, including:

1) Status of Contractor Activities; and

2) Status of Possible Delays;

iii) Review completed and/or cancelled change requests, for the past 36 consecutive months; and

iv) Reactivate and change a cancelled Change Request.

c) The Contractor must provide accounts for the Change Request Web service to all personnel identified by the Technical Authority per Schedule C: Response Targets for Change Management.

d) The Contractor must submit a monthly change report to the Client within 15 calendar days after the end of each month, commencing at the Client In-Service Date, which reflects its future planned activities, in accordance with Appendix E: Monthly Change Report.

3.2 Service Delivery

3.2.1 Planning Management

a) The Contractor must provide a detailed Planning Management processes to the Technical Authority no less than 40 calendar days after the contract award date.

b) The Contractor will meet with the Technical Authority on a quarterly basis to discuss mid to long-term planning activities, as it relates to, but is not limited to, power and space capacity requirements, in support of planned growth of the Contractor Facility.

c) The Contractor and the Client will work together to allow the two parties to minimize risk to the operating environment and the availability of the Client's IT computing equipment. The Technical Authority will provide a schedule of the critical business window to the Contractor no less than 30 calendar days before the Client In-Service Date specified in the contract, and updated by the Client on an annual basis and provided to the Contractor by September 30 of each year.

3.2.2 Service Level Management

a) The Contractor must submit a monthly service report to the Client within 15 calendar days after the end of each month starting the month immediately following the Client In-Service Date, in accordance with Appendix D: Monthly Service Report.

b) From the Client In-Service Date up to and inclusive of the first anniversary of the Client In-Service Date, the Contractor must meet with the Client each calendar month in person at a location in the NCA to be specified by the Technical Authority, to present the Monthly Service Report.

c) After the first anniversary of the Client In-Service Date, the Contractor must meet with the Client, at a location in the NCA to be specified by the Technical Authority, on a quarterly basis in the following months during the Period of the Contract:

   i) February

   ii) May

   iii) August

   iv) November

d) Following the monthly and quarterly meetings, the Contractor must provide draft minutes of the meeting, in accordance with Appendix C: Minutes of Meetings, to the Technical Authority no later than 7 calendar days after the status meeting has taken place.

e) The draft minutes of the meeting will be reviewed by the Technical Authority and if required by the Technical Authority, corrections or revisions will be noted and returned to the Contractor in no later than 7 calendar days.

f) The Contractor will have 7 calendar days after receiving the comments from the draft meeting minutes to make the necessary revisions and issue Final Minutes of the Meeting in electronic form (e.g. PDF) and distribute the document by e-mail to the Technical Authority and other representatives in attendance at the subject meeting.

3.2.3 Financial Management

a) The Contractor must provide monthly Expenditure Reports to the Technical and Contracting Authority indicating the total expenditure to date for each category identified in the Basis of Payment under the Contract. The Expenditure Reports must also include a summary of any changes in the co-location services, including any changes to, or deletions of, any of the services that form part of the Contract or any subsequent contract amendment. The reports must be provided monthly, with the first report due no later than the 15th of the month following Client In-Service Date and, thereafter, on the 15th day of each month, and will cover the previous calendar month.

3.2.4 Capacity Management

a) The Contractor must provide a detailed Capacity Management processes to the Technical Authority no less than 40 calendar days after the contract award date.

b) The Client's power consumption is expected to grow from 250 kVA to 1,000 kVA by April 30, 2015. Additional power of up to 1,000 kVA may be required to address unforeseen Client growth requirements during the contract period. Projected power consumption is provided for information purposes only.

c) The Client incremental power must be provided by the Contractor as follows:

Power Increment	Response Target
Greater than 0 kVA and less than or equal to 250 kVA	Provisioned in no more than 90 calendar days.
Greater than 250 kVA and less than or equal to 500 kVA	Provisioned in no more than 180 calendar days
Greater than 500 kVA and less than or equal to 1000 kVA	To be negotiated with the Contractor, with a target to provision in no more than 365 calendar days

d) If the Client power forecast projects a net decrease in Client Data Hall requirement, the Technical Authority reserves the right to request the Contractor to reduce the Client Data Hall configuration accordingly. In this event, the Contractor and the Technical Authority will work jointly to develop a plan to reduce the Client Data Hall configuration.

e) If the Client projects a net decrease in power, the Technical Authority reserves the right to reduce its previous contract year, annual average power consumption by 25 percent per year.

f) The Contractor must provide a monthly Contractor Facility Capacity Report within 15 calendar days following the end of each month, commencing at the Client In-Service Date, which itemizes, at a minimum, the following:

   i) Available and projected electrical capacity for the facility

   ii) Available and projected UPS electrical capacity

   iii) Available and projected building cooling capacity

   iv) Available and projected Client Data Hall cooling capacity

   v) Annualized data center Power Usage Effectiveness (PUE), where

$$\text{PUE} = \frac{\text{Total facility power}}{\text{IT equipment power}}$$

g) The Contractor must provide a monthly Client Capacity Report within 15 calendar days following the end of each month, which itemizes, at a minimum, the following:

   i) Client Electrical Usage (measured at the PDU)

   ii) Client UPS Electrical Capacity

   iii) Client Cooling Usage

   iv) Data Hall Floor Space Usage

   v) Data Hall Floor Space Availability

3.2.5 Availability Management

a) The Contractor must provide a detailed description of the Contractor Facility Monitoring processes and services to the Technical Authority no less than 40 calendar days after the contract award date.

b) The Contractor must monitor the Contractor Facility at all times including but not limited to the security systems, power systems, cooling systems and fire suppression systems.

c) The security systems, power systems, cooling systems and fire suppression systems must automatically generate alert notifications to the Contractor Facility Monitoring services.

3.3 Security

3.3.1 Security Management

a) The Contractor must provide a detailed description of the Contractor Facility security processes to the Technical Authority no less than 40 calendar days after the contract award date.

b) The Technical Authority will provide to the Contractor a list of client authorized personnel a minimum of 14 calendar days prior to the Client Fit-up Date specified in the contract.

c) The Technical Authority will provide the Contractor with updates to the list of client authorized personnel at least 2 calendar days in advance of the effective date of each personnel identified on the list requiring access to the facility.

d) The Contractor must have secure processes in place for granting and revoking access rights to the Contractor Facility on a 7/24 basis, including access in emergency situations. These processes will be reviewed on a quarterly basis between the Contractor and the Technical Authority and/or delegated Client security officer. The Contractor must at no additional cost to the Client, implement all security process changes the Technical Authority deems necessary to maintain security compliance throughout the Contract Period.

e) The Contractor must maintain an electronic log of all personnel who entered and/or exited the Client Data Hall. The log must reflect the historical access to the Client Data Hall for no less than 180 calendar days. If requested, the Contractor must provide a report of all personnel who entered and/or exited the Client Data Hall within 2 hours from the time the request is made by the Client's Security Authority.

f) The Contractor must allow the Client to implement a Client-controlled key management system.

g) The Contractor must allow the Client or a third party as selected by the Client to conduct periodic security audits of the Contractor Facility at the Client's expense, using qualified Client security personnel or qualified security screened consultants to ensure all security requirements of the co-location service are met on an on-going basis. The security audit will include, but is not limited to:

   i) The Contractor's implementation of personnel screening requirements detailed in 2.1.8 d);

   ii) The Contractor's implementation of an Acceptable Use Policy detailed in 3.3.2 a); and

   iii) The Contractor's implementation of an Acceptable Customer Policy detailed in 3.3.2 c).

   The Contractor will fully cooperate and provide supporting documentation and/or resources at no cost to the Client. The final report will be shared with the Contractor including deficiencies identified through the security audit. Such deficiencies shall be managed and corrected in accordance with Schedule B: Response Targets for Security Incident Management or as agreed to in writing between the Contractor and the Client.

g) The Contractor must have procedures in place to meet the performance criteria identified in Schedule B: Response Targets for Security Incident Management.

3.3.2 Contractor Facility Clients

a) The Contractor must have an Acceptable Use Policy that at a minimum meets the requirements stated in Appendix F: Acceptable Use Policy.

b) The Contractor must include, in its contracts, the requirements set out in the Acceptable Use Policy with all customers at the Contractor Facility.

c) The Contractor must have an Acceptable Customer Policy for the facility. An Acceptable Customer Policy is defined as the minimum standard by which the Contractor may accept customers at the Facility in order to protect the interests of all clients. The Acceptable Customer Policy must, at a minimum, reject any customer whereby:

i) the customer or customer's personnel are directly or indirectly affiliated to regimes listed on the Canada Economic Sanctions list, or;

ii) the customer does not agree to all conditions of the Acceptable Use Policy stated in Appendix F: Acceptable Use Policy.

The Contractor can access the list of Canada Economic Sanctions at:

English

http://www.international.gc.ca/sanctions/index.aspx?lang=eng

French

http://www.international.gc.ca/sanctions/index.aspx?lang=fra

d) The Contractor must not impose any changes to the Client as a result of a new customer with a higher security profile, such as Top Secret requirements.

e) The Contractor agrees that the Client has the right to audit the Contractor to ensure all customers in the facility are compliant to the Acceptable Customer Policy.

f) The Contractor agrees that the Client has the right to audit the Contractor to ensure enforcement of the Acceptable Use Policy for all customers in the facility.

g) Any contravention of the Acceptable Use Policy will be logged as an Incident and subject to all requirements identified in Section 3.1.2, Incident Management.

3.4 Report Submission and Meeting Requirements

a) Unless otherwise specified, all reports submitted by the Contractor to the Technical Authority and/or Contracting Authority must be written in English unless jointly agreed to by the Contracting Authority and the Technical Authority and the Contractor.

b) Unless otherwise agreed, all reports submitted by the Contractor to the Technical Authority and/or Contracting Authority must be delivered in electronic PDF format, including a source version saved in the software used to create the report (preferably Microsoft Word or such other format as may be jointly agreed to by the Contracting Authority and the Technical Authority and the Contractor from time to time).

c) Unless otherwise agreed, all reports submitted by the Contractor to the Technical Authority and/or Contracting Authority must be delivered by email, or by other means agreed to by the Contracting Authority and the Technical Authority and the Contractor.

d) Unless otherwise specified, all meetings will be held by teleconference.

3.5 Contractor Resources

3.5.1 Security Guards

a) At a minimum, the Contractor must provide a security guard at the Contractor Facility, on a 24 hours a day, 7 days a week, 365 days a year (366 days in leap years), that meet the following requirements:

i) Security guards must be bonded and hold certified security credentials from security organizations that meet or exceed the security requirements specified in the contract.

ii) The security guards at the main entrance of the Contractor Facility must be located in a separate secure area (physical barrier) from the area where individuals enter the Contractor Facility.

iii) The security guards must enforce positive identification and authentication of all personnel entering the Contractor Facility.

1) All authorized individuals entering the Contractor Facility must be given, at a minimum, a security card with photo identification.

2) All visitors to the Contractor Facility must provide valid credentials with photo identification, and sign a visitor's log book. All visitors entering the Contractor Facility must be escorted by authorized personnel at all times.

iv) The electronic security log and the paper visitor's log must be kept, at a minimum, for 6 months, showing a record of all individuals who have entered and exited the Contractor Facility.

3.5.2 Account Support

a) The Contractor must provide an account executive that meets the following requirements:

i) Has a minimum of 5 years experience performing the role of the corporate representative of the Contractor, with the general authority to make decisions related to all aspects of contract delivery; and

ii) The account executive must attend the monthly status meetings in person or via teleconference.

b) The Contractor must provide an account manager that meets the following requirements:

i) Has a minimum of 5 years experience acting as the single point of contact for a customer(s) and is responsible for the day-to-day administration of the Contract; and

ii) The account manager must attend, in person, the monthly status meetings and other meetings as requested by the Crown;

3.5.3 Technical Support

a) The Contractor must provide a facilities manager that has a minimum of 5 years experience acting as the corporate representative of the Contractor dealing with all aspects of Client service delivery within the data centre facility.

b) The Contractor must provide a primary customer service engineer to act as the technical and engineering expert on the co-location service. This resource will meet with a designated contact, identified by the Client, monthly and otherwise as requested by the Crown.

c) The Contractor must provide technicians assigned to the co-location service to act upon service requests contemplated in Schedule A, Schedule B and Schedule C.

3.5.4 Service Implementation

a) The Contractor must provide a Service Implementation Project Manager who will act as the corporate representative of the Contractor with the Client for all aspects of service implementation, as detailed in Section 4.

4 Service Implementation Requirements

4.1 Project Management Plan

a) The Contractor must provide a Project Management Plan within 7 calendar days of contract award in accordance with Appendix B: Service Implementation Project Management Plan, which lists as a minimum, the Contractor's overall approach for meeting the Service Implementation requirements, the process for milestone tracking of the Service Implementation activities, and Contractor activities and deliverables associated with the Service Implementation.

4.2 Kick-off Meeting

a) A kick-off meeting chaired by the Contracting Authority will be held with the Contractor and its representatives and the Technical Authority, no later than 10 calendar days after the Contract Award Date.

b) The meeting will be held in the NCA with the date, time and location of the kick-off meeting to be provided to the Contractor in writing by the Contracting Authority no later than 5 calendar days after the Contract Award Date.

c) The purpose of the meeting is to review the schedule and deliverables.

4.3 Status Reporting and Meetings

a) The Contractor must submit a formal status report to the Technical Authority by the Friday of each week from the Contract Award Date in accordance with the format outlined in Appendix A: Service Implementation Weekly Status Report. The status report will be submitted electronically by email in English in Adobe PDF.

b) The Contractor must arrange and attend a Weekly Status Meeting no more than 3 calendar days after submitting the Weekly Status Report, with the Technical Authority and designated representatives, by teleconference, to provide an update on the overall progress of the Service Implementation activities in the Project Management Plan.

c) Following the weekly meeting, the Contractor must submit draft Minutes of the Meeting to the Technical Authority no later than 1 calendar day after the weekly status meeting has taken place in accordance with the format outlined in Appendix C: Minutes of Meetings. The Minutes of the Meeting will be submitted electronically via email in English in Adobe PDF.

d) The draft Minutes of the Meeting will be reviewed by the Technical Authority. If required, corrections or revisions will be noted and returned to the Contractor no later than 1 calendar day.

e) The Contractor will have 1 calendar day to make the necessary revisions required by the Technical Authority and issue the Final Minutes of the Meeting to the technical Authority, submitted electronically by email in English in Adobe PDF.

4.4 Establishment of Co-location Service

4.4.1 Location of Contractor Facility

a) The Contractor must provide a single co-location service to be used by the Client, in the range of not less than 10 kilometres in straight line distance from Angus, Ontario (Latitude, Longitude: (44.313872, -79.8842912)), and not more than 100 kilometres of fibre installed network distance as measured from Angus, Ontario (Latitude, Longitude: (44.313872, -79.8842912)) . This condition is necessary to meet the following 2 imperative operational requirements for the Clients:

   i) Minimum geographic separation between the existing Client data centre located at CFB Borden, Ontario, Canada to reduce the risks of both the Client's data centre and the Contractor's facility being out of service at the same time; and

   ii) Maximum distance between the Contractor Facility and the Client's data centre to permit high-speed synchronous telecommunications interconnectivity, as limited by the Client's current IT applications, IT infrastructure and network technology configurations.

b) The Contractor must provide the co-location service using a primary source of hydro from a substation that is independent from the hydro service used at Angus, Ontario.

c) The Contractor must deliver the service from a Contractor Facility and location that minimizes the impact of potential hazardous situations, such as but not limited to a flood plain, railway or highway used to transport hazardous materials, and adjacent uses, including but not limited to chemical plants and chemical warehouses.

4.4.2 Conditions for Contractor Facility

a) The Contractor's facility must meet or be equivalent to the Uptime Institute (UTI) Tier III Topology for data centres. Tier III requirements are defined by Uptime Institute in the Data Centre Site Infrastructure Tier Standard: Topology (Appendix H). The Contractor's facility will be validated against the Uptime Institute Topology by an independent Uptime Institute accredited third party chosen by Canada.

b) The Contractor must allow the Client or a third party as selected by the Client to conduct periodic validation of the Contractor Facility at the Client's expense, using qualified Client personnel or qualified screened consultants to ensure all UTI equivalency requirements of the co-location service are met on an on-going basis.

c) The Contractor must provide the service from a standalone facility dedicated for the exclusive purpose of data centre services.

d) The Contractor must deliver the service from a facility without exterior or interior visible signage that would disclose either the purpose of the Contractor Facility or the identity of the Clients using the Contractor Facility.

e) The Contractor must obtain all necessary third-party approvals and licenses in compliance with all applicable laws so that the co-location site is deemed fully operational and occupant ready no later the Ready For-Use Date.

f) The Contractor must provide the Client with the rights to install and access satellite dishes in order to support satellite services to the Client Data Hall.

g) The Contractor Facility must provide a general parking area, with a minimum of 4 parking spots, for use by the Client at no additional charge to the Client.

4.4.3 Data Hall Requirements

a) The Client will provide a profile of the Client Computing Equipment (CCE) to the Contractor no less than 5 days after the contract award date.

b) The Contractor must develop the design of the Client Data Hall with review by the Client, from the time the CCE profile is provided, to ensure all client technical issues are being fully addressed. The Data Hall design must support the CCE in accordance with requirements identified in Section 2.2.3 Power Requirements (a) and (b). The Data Hall design must include, but is not limited to:

   i) Development of Client Data Hall cabinet floor plan;

   ii) Power distribution design;

   iii) Cooling design; and

   iv) Cable plant design.

c) The Contractor must submit the Client approved Client Data Hall design to the Client no less than 15 days after the contract award date.

d) The Contractor will work jointly with the Client to complete the Data Hall configuration based on the approved design. The Client Data Hall configuration will include, but is not limited to:

   i) Provision and installation of cabinets including CPDUs;

   ii) Provision and installation of power to the Client cabinets and stand alone equipment;

   iii) Provision and installation of cooling to the Client cabinets and stand alone equipment;

   iv) Provision and installation of network cabling to the Client cabinets and stand alone equipment;

   v) Provision and installation of cable management trays.

e) The Client Data Hall must be ready for use no less than 30 days after the contract award date.

f) The Client Data Hall and cabinets must be cleaned and free of all construction materials and debris.

4.5 Acceptance Requirements

4.5.1 Client Data Hall Construction

a) Client Security Officers must review the Contractor's blueprints for the Client Data Hall at the 33%, 66% and 99% stages, to ensure that the security requirements in Section 2.1.8 have been properly addressed

b) Client Security officers will carry out acceptance testing of the Radio Frequency Shielding as detailed in the Communications Security Establishment Canada (CSEC) document ITSG-02 found at:

English

http://www.cse-cst.gc.ca/its-sti/publications/itsg-csti/itsg02-eng.html

French

http://www.cse-cst.gc.ca/its-sti/publications/itsg-csti/itsg02-fra.html

4.5.2 Client Data Hall Acceptance Testing Procedure

c) Thirty (30) calendar days after the contract award date when the contractor has declared the Client Data Hall ready for use, the Contractor must provide 15 consecutive calendar days, for the Client to conduct acceptance testing of the Data Hall

d) The Client will provide a test plan to the Contractor 15 calendar days prior to Client Data Hall acceptance testing.

e) The Contractor will, at that time, allow the Client to deliver a representative set of IT equipment and cabinets (as required), to the Contractor's site it will use to conduct its testing.

f) The Contractor will uncrate and move the Client equipment into the Client's Data Hall.

g) The Client will install it's computing equipment into the cabinets and standalone configurations as required;

h) The Client acceptance test will consist of, but is not limited to:

i) Testing of network connections;

ii) Testing of dual power bus;

iii) Data Hall construction; and

iv) Data Hall access mechanisms.

i) All items found by the Client not to be compliant with the contract will be documented by the Client. A paper copy of the document will be delivered to the Contractor and the Contract Authority no more than 5 calendar days after completion of the Client Data Hall acceptance testing.

j) The Contractor will have 10 calendar days to correct all items found to be not compliant by the Client. The Contractor must provide documented evidence to the Client that each item has been corrected. The Client may at its sole discretion retest and conduct Client Data Hall

acceptance testing as a result of the documentation provided by the Contractor until such time it is satisfied that the requirements have been met.

k) The Client will provide a paper copy of the Client Data Hall acceptance document to the Contractor and the Contract Authority no more than 10 calendar days following a successful test.

4.5.3 Client Transition Planning

Transition is defined as those activities which will be provided by the Contractor to establish Client IT services within the Contractor Facility.

a) The Contractor must provide a Transition Plan Template no less 40 calendar days after the contract award date. A Transition Plan Template outlines as a minimum the overall approach and typical activities associated with the migration of the Client IT equipment from the Client location(s) to the Contractor Facility, including but not limited to, Client Data Hall design and configuration, installation, testing, and initial operation. The Transition Plan must be coordinated with the Client Migration plan.

b) The Contractor will arrange an initial Transition Planning meeting with the Client to begin the development of the Transition Plan no less than 45 calendar days after the contract award date.

c) The Contractor will work jointly with the Client to create the Transition Plan immediately upon the initial meeting, updating as required and producing revised plans on a 5 calendar day cycle. The Transition Plan must be coordinated with the Client Migration Plan until the completion of all Client Migration activities.

d) The Contractor will produce the final Transition Plan not less than 60 calendar days after the contract award date, outlining, but not limited to, the following activities:

   i) Contractor Responsible Activities:

      1) Development of transition schedule;

      2) Development of the Client equipment layout;

      3) Testing the power connections;

      4) Testing of network connections from the telecommunications point of presence to the Client Data Hall

      5) Secure temporary storage of Client equipment, as required;

      6) Un-crating the Client equipment;

      7) Disposing of the crating materials; and

      8) Moving the Client equipment to the Client Data Hall.

4.5.4 Client Fit-up

Client Fit-up is defined as the activities which the Client will perform to establish the Client's IT infrastructure in the Client Data Hall. This work will commence no later than 70 calendar days after contract award.

a) Client Responsible Activities:

1) Client review and approval of equipment layout;
2) Client review and approval of schedule;
3) Network design;
4) Installation and fit-up of network to the Client cabinets and stand alone equipment;
5) Testing network connections in the Client Data Hall;
6) Delivery of equipment to site;
7) Installing the Client computing equipment into the cabinets; and
8) Testing the installed Client equipment connectivity.

NOTE: The above stated timelines associated with Service Implementation Requirements are the responsibility of the Contractor and the Client. Any Canada imposed delays will cause adjustment to the subsequent timelines.

5 Other Base Services

In accordance with the Pricing Tables, the Contractor must provide all services to carry out the following requirements:

a) The Contractor must provide and install data centre cabinets and cabinet power distribution units (CPDU) for Client computing equipment (refer to 5b below for specifications). The cabinet installation will include:

   i) Power, which consists of circuits, circuit cabling and circuit receptacles as required;

   ii) Cooling, which consists of air containment, blanking panels, venting and any other components required to cool the Client's IT equipment as dictated by the Contractor's cooling solution.

b) The contractor must provide cabinets and CPDUs that meet the following minimum specifications:

Item	Configuration
Server cabinets – 42U	Inclusive of all venting and air flow additions, side panels, cable management components, cable trays, seismic bracing, rails and lockable doors with unique key sets. 30"w x 42"d x 84"h
Network cabinets – 42U	Inclusive of all venting and air flow additions, side panels, cable management components, cable trays, seismic bracing, rails and lockable doors with unique. 30"w x 42"d x 84"h 40"w x 42"d x 84"h
CPDU	Support a minimum of 12 x C13 and 12 x C19 IEC receptacles; IP addressable with support of Simple Network Management Protocol (SNMP) access for remote power reset and power consumption monitoring.

The cabinet and CPDU standard models deployed by the Contractor will be used by the Client to direct the vendor community on the standard for factory cabinet mounted and configured, integrated computing platforms;

c) The Contractor must install in the data hall, Client standalone equipment that is proprietary and does not conform to the standard cabinet and CPDU configurations. This Client equipment may require the Contractor to address specific cooling considerations, as well as, dedicated power circuits and cabling requirements, including 3phase 208V. The Client IT infrastructure is estimated to consist of 90% cabinet mount equipment and 10% standalone equipment.

d) Provision and installation of cable management trays within the Client Data Hall such that all network and power cables terminate at the Client cabinets or Client non-rackable equipment;

e) Provision and installation of network cabling to the Client Data Hall network termination point;

f) The Contractor must perform cabling services, based on the Client cable plant architecture, which will include the provisioning and installation of required materials, for, but not limited to, the following:

iii) provide a network cabling configuration that conforms to the most recent TIA-942 Telecommunications Infrastructure Standard for Data Centres;

iv) Installation of Unshielded Twisted Pair (UTP) and fibre optic cables;

v) Perform connections of Ethernet Local Area Networks (LAN) over UTP and/or fibre optic cabling and equipment;

vi) Create specific installation plans, providing implementation schedules, costing analysis, and progress reports;

vii) Install and test UTP and fibre LAN backbone. Install and test horizontal distribution and cross connects, perform conduit and cable tray planning;

viii) Moves, Adds, and Changes (MAC) – day to day requirements, as well as larger relocations of data equipment, as they apply to cable systems;

ix) Repairs – replacement or repair of damaged cabling components and restoration of connectivity;

x) Upgrades – to existing cable systems where operational requirements dictate;

xi) Records and Drawings – update existing electronic cabling records and drawings as required and as changes to the cabling system are made by the cabling contractor;

g) Testing of network connections to confirm point to point connectivity from the telecommunication rooms to the Client termination point; and

h) Electrician services as required by the Client to install or reconfigure electrical circuits in accordance with OEM guidelines.

6 Optional Services

In accordance with the Pricing Tables, the Contractor must, when requested to do so, provide all services to carry out the following requirements:

6.1 Equipment Support Services

a) The Contractor must be available at all times to provide:

i) server reboot and/or power cycling services for Client IT equipment within 30 minutes of a Client request; and

ii) visual monitoring service to check server indicator lights within 30 minutes of a Client request;

6.2 Co-location Space Management

6.2.1 Installation of Client Computing Equipment

a) The Contractor must install the Client's computing equipment into cabinets or in standalone configurations.

b) The Contractor must test the Client's computing equipment to ensure that the equipment can power on successfully.

6.2.2 Removal of Client computing equipment

a) The Contractor must provide removal services of the Client's computing equipment from cabinets or standalone configurations from within the Client Data Hall to the Temporary Secure Storage Area or loading dock as directed by the Client.

Schedule A: Response Targets for Incident Management

The following table identifies the minimum requirements that the Contractor and Client will use to identify and manage incidents at the Contractor Facility.

An **incident** is any event which causes, or may cause, an interruption to, or a reduction in the quality of the service.

The **incident impact** is defined as the measure of the business criticality of an incident or problem, and the urgency is the necessary speed of responding.

A **problem** is the unknown underlying cause of one or more incidents. A problem becomes a known error when the root cause is known and a workaround or permanent solution has been identified.

Priority	Description	Response
1 – Critical	Client Service Outage • Incidents characterized by an actual or imminent failure to the Contractor Facility, where the Client is (or will be) experiencing any level of outage to any of the Client IT equipment.	• The Contractor must notify the Client's help desk within 15 minutes upon occurrence of the incident • The Contractor must resolve the problem within 2 hours from the start of the occurrence of the incident. • The Contractor must provide a resolution status update to the Technical Authority on a 30-minute basis until the problem is resolved • Once the problem has been resolved, the Contractor must document the incident and associated resolution, and send a copy of the document to the Technical Authority within 7 calendar days of the resolution. • The change required to resolve the incident must be recorded as an unplanned change in the Change Management System

Priority	Description	Response
2 - High	Client Service Degradation • Incidents characterized by an actual or imminent failure to the Contractor Facility, where the Client is (or will be) experiencing a complete loss of redundancy of any component of the co-location service resulting in risk of outage to any of the Client IT equipment.	• The Contractor must notify the Client's help desk within 30 minutes upon occurrence of the incident • The Contractor must resolve the problem within 8 hours from the start of the occurrence of the incident. • The Contractor must provide a resolution status update to the Technical Authority on an hourly basis from the start of the occurrence until the problem is resolved • Once the problem has been resolved, the Contractor must document the incident and associated resolution, and send a copy of the document to the Technical Authority within 7 calendar days of the resolution
3 – Medium	Service Degradation Incidents where any contractual service level is not achieved, and is not directly related to the Client Data Hall.	• The Contractor must notify the Client's help desk within 60 minutes upon occurrence of the incident • The Contractor must resolve the problem within 24 hours from the start of the occurrence of the incident • The Contractor must provide a resolution status update to the Technical Authority on a 6-hour basis until the problem is resolved • Once the problem has been resolved, the Contractor must document the incident and associated resolution, and provide the information as part of the Monthly Status Report
4 - Low	Issue • Incidents characterized by no degradation in service and no impact to Client IT equipment	• The Contractor must notify the Client's help desk within 12-hours upon the occurrence of the incident • The Contractor must resolve the problem within 7 calendar days from the start of the occurrence of the incident • The Contractor must provide a resolution status update to the Technical Authority as requested until the problem is resolved • Once the problem has been resolved, the Contractor must document the incident and associated resolution, and provide the information as part of the Monthly Status Report

Schedule B: Response Targets for Security Incident Management

The following table identifies the minimum requirements that the Contractor and Client will use to identify and manage security incidents at the Contractor Facility.

Priority	Description	Performance Indicators
1 – Critical	Critical Security Incident • Security Incidents resulting in the Client experiencing any level of outage to any of the Client IT equipment.	• The contractor must respond to a Critical Priority Incident as per Schedule A – Response Targets for Incidents • The Contractor must convene a meeting with the Client within 7 calendar days of the security incident to discuss the incident, and all measures being taken by the Contractor to ensure that any future similar incidents can be prevented.
2 – High	High Security Incident • Security incidents resulting in a risk of compromise to any of the Client IT equipment or Client applications.	• The contractor must respond to a High Priority Incident as per Schedule A – Response Targets for Incidents • The Contractor must convene a meeting with the Client within 7 calendar days of the security incident to discuss the incident, and all measures being taken by the Contractor to ensure that any future similar incidents can be prevented.
3 – Medium	Medium Security Incident • Security incident resulting in unauthorized access to any secured area. • No Client service failure	• The contractor must respond to a Medium Priority Incident as per Schedule A – Response Targets for Incidents • The Contractor must convene a meeting with the Client within 7 calendar days of the security incident to discuss the incident, and all measures being taken by the Contractor to ensure that any future similar incidents can be prevented.
4 – Low	Low Security Incident • General security breaches, not including access to the Client Data Hall. • No Client service failure	• The contractor must respond to a Low Priority Incident as per Schedule A – Response Targets for Incidents

Schedule C: Response Targets for Change Management

The following table identifies the minimum requirements that the Contractor and Client will use to identify and manage changes at the Contractor Facility.

Priority	Description	Performance Indicators
Priority 1 Unplanned Emergency Change	Any unplanned emergency change requested by the Contractor. The change may cause one or more clients to experience degradation in service. The change may be to resolve a problem related to any of the following: • Schedule A incident of priority 1, 2 or 3. • Schedule B security incident of priority 1, 2 or 3.	• The Contractor must notify the Client's help desk within 15 minutes of the change request that they have initiated. • The Contractor must implement the change within the subsequent 24 hours of the change request. • The Contractor must seek approval where feasible from all Clients that are at risk of degradation or further disruption in service as a result of the change. • The Contractor must provide the Technical Authority with a post mortem report no less than 3 calendar days following the unplanned change. • The Contractor must document the change in accordance with Appendix E – Minimum Requirements for Monthly Change Report.
Priority 2 Urgent Change	Any planned or unplanned urgent change requested by the Contractor. The change may cause one or more clients to experience degradation in service. The change may be to resolve a problem related to any of the following: • Schedule A incident of priority 2 or 3. • Schedule B security incident of priority 2 or 3.	• The Contractor must notify the Client's helpdesk within 30 minutes of the change request that they have initiated. • The Contractor must implement the change within the subsequent 7 calendar days of the change request. • The Contractor must obtain approval from all clients that are at risk of degradation or further disruption in service as a result of the change. • The Contractor must provide the Technical Authority with a post mortem report no less than 7 calendar days following the change. • The Contractor must document the change in accordance with Appendix E – Minimum Requirements for Monthly Change Report.

Priority	Description	Performance Indicators
Priority 3 Normal Change	Any planned or unplanned normal change requested by the Contractor or the Client. The change may cause one or more clients to experience degradation in service. The change may be to resolve a problem related to any of the following: • Schedule A incident of priority 2 or 3. • Schedule B security incident of priority 2 or 3.	• The Contractor and the Client must notify each other within 24 hours of the change request that they have initiated. • The Contractor must implement the change within the subsequent 30 calendar days of the change request or as agreed to with the Client. • The Contractor must obtain approval from all clients that are at risk of degradation or further disruption in service as a result of the change. • The Contractor must document the change in accordance with Appendix E – Minimum Requirements for Monthly Change Report.
Priority 4 Short-term Planned Change	Any short-term planned change requested by the Contractor or the Client	• The Contractor and the Client must notify each other within 14 calendar days of the change request that they have initiated. • The Contractor will implement the change in no less than 3 months and no more than 6 months of the change request. • The Contractor must obtain approval from all clients that are at risk of degradation or further disruption in service as a result of the change. • The Contractor must document the change in accordance with Appendix E – Minimum Requirements for Monthly Change Report.
Priority 5 Long-term Planned Change	Any long-term planned change requested by the Contractor or the Client	• The Contractor and the Client must notify each other within 14 calendar days of the change request that they have initiated. • The Contractor will implement the change in no less than 6 months of the change request. • The Contractor must obtain approval from all clients that are at risk of degradation or further disruption in service as a result of the change. • • The Contractor must document the change in accordance with Appendix E – Minimum Requirements for Monthly Change Report.

Priority	Description	Performance Indicators
Priority 6 Information Change	Any information change requested by the Contractor or the Client. The change will not result in any risk or disruption to Client service. The change may be related, but not limited to: • Change in Contractor personnel list • Change in Technical Authority contact list • Request for account to incident, problem or change management systems.	• The Contractor and the Client must notify each other immediately of the change request that they have initiated. • The Contractor must implement the change within the subsequent 7 calendar days of the change request. • The Contractor must document the change in accordance with Appendix E – Minimum Requirements for Monthly Change Report.

Appendix A: Service Implementation Weekly Status Report

The following are minimum requirements for the Service Implementation Weekly Status Report:

1 Introduction
2 Scope
3 Objective
4 Background
5 Overview
6 Project Information
  6.1 Project Name
  6.2 Phase
  6.3 Plan Start Date
  6.4 Plan End Date
  6.5 Project Manager
7 Project Current Phase Information
  7.1 Accomplishments in the reporting period
  7.2 Planned activities for the next reporting period
  7.3 Unplanned activities (completed or anticipated)
8 Issues and Problems Requiring Attention or Action
  8.1 Project Issues
    8.1.1 Issue Description
    8.1.2 Status
    8.1.3 Proposed Resolution
    8.1.4 Planned Resolution Date
    8.1.5 Revised Resolution Date
    8.1.6 Actual Resolution Date
  8.2 Risks
    8.2.1 Risk Number
    8.2.2 Risk Description
    8.2.3 Probability
    8.2.4 Impact
    8.2.5 Mitigation
    8.2.6 Residual Risk
  8.3 Schedule Slippage Report
    8.3.1 Activity
    8.3.2 Reason for Slippage
    8.3.3 Impact of Slippage
    8.3.4 Action to remedy slippage
    8.3.5 Schedule Impact

Appendix B: Service Implementation Project Management Plan

The following are minimum requirements for the Service Implementation Project Management Plan:

1 Project Overview
- 1.1 Introduction
- 1.2 Project Strategy
- 1.3 Purpose, Scope, and Objectives
- 1.4 Assumptions and Constraints
- 1.5 Definitions and Acronyms

2 Project Organization
- 2.1 Description of Management Structure
- 2.2 Description of Project Management Team

3 Work Plan
- 3.1 General Description
- 3.2 Major Milestones and Schedule
  - 3.2.1 Proof of New or Retrofit Building Permit
  - 3.2.2 Design reviews at 33%,66%,99%
  - 3.2.3 Client Security Review
  - 3.2.4 Uptime Certification of Design Documents
  - 3.2.5 Building Permit
  - 3.2.6 Completion of Building Shell (roof and exterior walls up)
  - 3.2.7 Building connected to Hydro Grid
  - 3.2.8 Major electrical components delivered to site (UPS, Generator, PDUs)
  - 3.2.9 Major Mechanical systems delivered to site (A/Cs or Chillers, Heat wheel)
  - 3.2.10 Telecommunication carriers network terminated in Telecommunications rooms
  - 3.2.11 Computer room ready for commissioning
  - 3.2.12 Occupancy permit
  - 3.2.13 All systems commissioned
  - 3.2.14 Ongoing security review checkpoints
  - 3.2.15 Contractor Testing
  - 3.2.16 Uptime Certification of Tier III
  - 3.2.17 Client Testing
  - 3.2.18 LEED Certification
  - 3.2.19 Approval of Client Transition Plan

4 Project Tracking Plan
- 4.1 Requirements Management
- 4.2 Schedule Control
- 4.3 Quality Control

5 Risk Management Plan
- 5.1 List of Risks
  - 5.1.1 Description of Risk
  - 5.1.2 Description of Impact of Risk
  - 5.1.3 Probability Assessment
  - 5.1.4 Risk Assessment
  - 5.1.5 Mitigation Strategies

6 Client Commissioning, Testing Plan, and Transition Plan
- 6.1 Development of Client Data Hall design and space layout.
- 6.2 Development of transition schedule
- 6.3 Installation and fit-up (power and network) of the Client cabinets and stand alone equipment

6.4 Testing the power connections
6.5 Testing network connections
6.6 Installing the Client computing equipment into the cabinets
6.7 Testing the installed Client equipment connectivity

Appendix C: Minutes of Meetings

The following are minimum requirements for the Minutes of Meetings:

1 Title of Meeting
2 Date of Meeting
3 Time of Meeting
4 Attendees
5 Absentees
6 Minutes Taken By
7 Copy of Minutes Sent To
8 Minutes of Discussions
9 Record of Decisions Taken
10 Action Items Raised
11 Other Business
12 Next Meeting
13 Appendix - Action Items List
- 13.1 Overview
- 13.2 Number of the action item
- 13.3 Description of the action item
- 13.4 Person responsible for following through (OPI)
- 13.5 Date initiated
- 13.6 Date due
- 13.7 Comments

Appendix D: Monthly Service Report

The following are minimum requirements for the Monthly Service Report for the Client in-service contract period:

1 Summary of Incidents
  1.1 Overall Summary
    1.1.1 Total Number of Incidents
    1.1.2 Number of Incidents by Severity
2 Summary of Problems
  2.1 Overall Summary
    2.1.1 Total Number of Problems
    2.1.2 Number of Problems by Severity
3 Summary of Resolutions
  3.1 Problem Description
  3.2 Problem Severity
  3.3 Description of Resolution
  3.4 Turnaround Time to Resolution
4 Summary of Changes
  4.1 Change Description
  4.2 Change Severity
  4.3 Result of Change
5 Service availability
6 Service reliability
7 Service capacities
  7.1 Power usage, both aggregate and by circuit
  7.2 Floor space use
  7.3 Cooling use, both aggregate and by Client Data Hall
8 Service thresholds that initiate service expansion
9 Future plans for both Contractor and the Client

Appendix E: Monthly Change Report

The following are minimum requirements for the Monthly Change Report for the Client in-service contract period:

1 Summary of Unplanned Contractor Changes (Completed)
- 1.1 Overall Summary
  - 1.1.1 Total Number of Unplanned Changes
  - 1.1.2 Number of Unplanned Changes by Severity
  - 1.1.3 Detail Unplanned Change List
    - 1.1.3.1 Description
    - 1.1.3.2 Severity
    - 1.1.3.3 Result of Unplanned Change

2 Summary of Planned Contractor Changes (Completed)
- 2.1 Overall Summary
  - 2.1.1 Total Number of Planned Changes
  - 2.1.2 Number of Planned Changes by Severity
  - 2.1.3 Detail Planned Change List
    - 2.1.3.1 Description
    - 2.1.3.2 Severity
    - 2.1.3.3 Result of Planned Change

3 Summary of Planned Client-Requested Changes (Completed)
- 3.1 Overall Summary
  - 3.1.1 Total Number of Planned Changes
  - 3.1.2 Number of Planned Changes by Severity
  - 3.1.3 Detail Planned Change List
    - 3.1.3.1 Description
    - 3.1.3.2 Requestor
    - 3.1.3.3 Severity
    - 3.1.3.4 Result of Planned Change

4 Summary of Planned Contractor Changes (Future)
- 4.1 Overall Summary
- 4.2 Total Number of Planned Changes
- 4.3 Number of Planned Changes by Severity
- 4.4 Detail Planned Change List
- 4.5 Description
- 4.6 Severity
- 4.7 Result of Planned Change

5 Summary of Planned Client-Requested Changes (Future)
- 5.1 Overall Summary
  - 5.1.1 Total Number of Planned Changes
  - 5.1.2 Number of Planned Changes by Severity
  - 5.1.3 Detail Planned Change List
    - 5.1.3.1 Description
    - 5.1.3.2 Requestor
    - 5.1.3.3 Severity
    - 5.1.3.4 Result of Planned Change

Appendix F: Acceptable Use Policy

All customers of the co-location data centre must agree and adhere to an Acceptable Use Policy (AUP) which must, at a minimum, include the following conditions:

(a) The customer must only use services supplied by the Contractor for lawful purposes;
(b) The customer may not transmit, retransmit, redirect, display, or store material in violation of any applicable laws (including rights protected by copyright, trade secret, patent or other intellectual property or similar laws or regulations), industry or community standards. This includes, but is not limited to material that is; obscene, indecent, defamatory, libelous, racist, or threatening;
(c) The customer may not engage in activity that may or will interfere with the service of another user, host or network;
(d) The customer may not engage in the distribution of software, programs or messages that may cause damage or annoyance to persons, data, and/or computer systems;
(e) The customer may not engage in fraudulent activities including, but not limited to, intentional misrepresentations or misleading statements, writings or activities made with the intent that the person receiving it will act upon it; obtaining services with the intent to avoid payment; and hosting of phishing websites;
(f) The customer is prohibited from activity considered a precursor to attempted security violations including, but not limited to, any form of scanning, probing, or other testing or information gathering activity;
(g) The customer may not attempt to penetrate security measures of other systems;
(h) The customer may not attempt unauthorized access including illegal, unauthorized access to, or attempt to access, other computers, accounts, networks or systems;
(i) The customer may not introduce any prohibited item into the data center (raised floor area). Prohibited items include, but are not limited to, the following:
    - combustible materials (i.e. cardboard)
    - food and drink
    - explosives and weapons
    - hazardous materials
    - alcohol, illegal drugs and other intoxicants
    - electro-magnetic devices
    - radioactive materials
    - cameras or any other recording device;
(j) The customer may not store any materials in the Client Data Hall (other than equipment manuals);
(k) The customer may not store any materials in common areas (i.e. hallways or loading dock);
(l) The customer may not lift raised floor tiles or penetrate walls;
(m) The customer may not take pictures without express written consent by the Facility Manager; and
(n) The customer may not sub-let or otherwise allow usage of its space to other organizations or individuals who are not explicitly named in the Customer's contract or where the Customer does not have full legal responsibility.

Appendix G: List of Acronyms and Applicable Documents

Acronym	Description
CCE	Client Computing Equipment
CFO	Chief Financial Officer
CIO	Chief Information Officer
DCFS	Data Centre Feasibility Study
DG	Director General
CEPA	Canadian Environmental Protection Agency
GC	Government of Canada
HVAC	Heating, Ventilating and Air Conditioning
IT	Information Technology
km	Kilometre
kVA	Kilo Volt Amperes
LAN	Local Area Network
LEED	Leadership in Energy and Environmental Design
MAC	Moves, Adds and Changes
MW	Megawatts
NCA	National Capital Area
PDU	Power Distribution Unit
PM	Product Management (ITSB Sector)
PMP	Project Management Plan
PUE	Power Usage Effectiveness
RFU	Ready For Use
CPDU	Cabinet Power Distribution Unit (power bar)
SMS	Shared Metropolitan Services
SNMP	Simple Network Management Protocol
SSC	Shared Service Canada
TIA	Telecommunications Industry Association
UTP	Unshielded Twisted Pair
VA	Volt Amperes
WBS	Work Breakdown Structure

Appendix H: Uptime Institute Tier Standard Topology

Note to Bidders:

Document “Data Center Site Infrastructure Tier Standard: Topology” follows.

Appendix I: Security Requirements

Note to Bidders:

Document “G13-01 Secure Storage Rooms” and Document “G13-02 Secure Demising Wall” follows.

UPTIME INSTITUTE, LLC

Data Center Site Infrastructure Tier Standard: Topology

Prepared by Uptime Institute Professional Services, LLC

20 West 37th Street - 6th Floor
New York, NY 10018

Uptime Institute™ LLC

Abstract: The Institute *Tier Standard: Topology* is an objective basis for comparing the functionality, capacity, and expected availability (or performance) of a particular site infrastructure design topology against other sites, or for comparing a group of sites. This Standard describes criteria to differentiate four classifications of site infrastructure topology based on increasing levels of redundant capacity components and distribution paths. This Standard focuses on the definitions of the four Tiers and the performance confirmation tests for determining compliance to the definitions. The Commentary, in a separate section, provides practical examples of site infrastructure system designs and configurations that fulfill the Tier definitions as a means to clarify the Tier classification criteria.

Keywords: ambient temperatures, autonomous response, availability, classification, Compartmentalization, Concurrent Maintenance, Concurrently Maintainable, Continuous Cooling, data center, dry bulb, dual power, Fault Tolerance, Fault Tolerant, functionality, infrastructure, metrics, Operational Sustainability, performance, redundant, reliability, Tier, Tier level, Tiers, topology, wet bulb

Introduction

This introduction is not part of the Institute *Data Center Site Infrastructure Tier Standard: Topology*. It provides the reader with context for the application of the Standard.

This Institute *Data Center Site Infrastructure Tier Standard: Topology* is a restatement of the content previously published as the Institute publication *Tier Classifications Define Site Infrastructure Performance*. Selected content of this publication has been reedited into an ANSI Standards Model format. Future updates or changes to the Institute *Tier Standard: Topology* shall be accomplished through a review and recommendation process consistent with other recognized Standards bodies.

The Tier Classifications were created to consistently describe the site-level infrastructure required to sustain data center operations, not the characteristics of individual systems or subsystems. Data centers are dependent upon the successful and integrated operation of electrical, mechanical, and building systems. Every subsystem and system must be consistently deployed with the same site uptime objective to satisfy the distinctive Tier requirements. The most critical decision-making perspective owners and designers must consider, when making inevitable tradeoffs, is what effect does the decision have on the life-cycle-integrated operation of the Information Technology (IT) environment in the computer room.

Simply put, the Tier topology rating for an entire site is constrained by the rating of the weakest subsystem that will impact site operation. For example, a site with a robust Tier IV UPS configuration combined with a Tier II chilled water system yields a Tier II site rating.

This very stringent definition is driven by senior executives who have approved multi-million dollar investments for an objective report of actual site capabilities. Any exceptions and exclusions footnoted in the approval documents will be quickly lost and forgotten. If a site has been advertised within an organization as being Fault Tolerant (Tier IV), it will be inconsistent to have to plan a site shutdown at any time in the future—regardless of any "fine print" exclusions that diligently identified the risk. For this reason, there are no partial or fractional Tier ratings. A site's Tier rating is not the average of the ratings for the critical site infrastructure subsystems. The site's Tier rating is the lowest of the individual subsystem ratings.

Similarly, the Tier rating cannot be claimed by using calculated mean time between failures (MTBF) component statistical reliability to generate a predictive availability and then using that number to match the empirical availability results with those of sites representing the different Tier classifications. Statistically valid component values are not available, partly because product life cycles are getting shorter and no independent, industry-wide database exists to collect failure data.

Finally, this Standard focuses on the topology and performance of an individual site. High levels of end-user availability may be attained through the integration of complex IT architectures and network configurations that take advantage of synchronous applications running on multiple sites. However, this Standard is independent of the IT systems operating within the site.

Copyrights

Participants

The original contents of the *Data Center Site Infrastructure Tier Standard: Topology* were developed by the following individuals:

W. Pitt Turner, IV John H. Seader Vincent E. Renaud

With editorial contribution by:

Julian S. Kudritzki Kenneth G. Brill

Contents

1. Overview

1.1 Scope

This Standard establishes four distinctive definitions of data center site infrastructure Tier classifications (Tier I, Tier II, Tier III, Tier IV), and the performance confirmation tests for determining compliance to the definitions. The Tier classifications describe the site-level infrastructure topology required to sustain data center operations, not the characteristics of individual systems or subsystems. This Standard is predicated on the fact that data centers are dependent upon the successful and integrated operation of several separate site infrastructure subsystems, the number of which is dependent upon the individual technologies (e.g., power generation, refrigeration, uninterruptible power sources, etc.) selected to sustain the operation.

Every subsystem and system integrated into the data center site infrastructure must be consistently deployed with the same site uptime objective to satisfy the distinctive Tier requirements.

Compliance with the requirements of each Tier is measured by outcome-based confirmation tests and operational impacts. This method of measurement differs from a prescriptive design approach or a checklist of required equipment.

Commentary on this Standard is in a separate section that provides examples for the design and configuration of facility systems for each Tier topology level. The commentary section also offers guidance in the application and implementation of the Tier definitions. In addition, the commentary section includes discussion and examples to aid in understanding Tier concepts as well as information on common design topology shortfalls.

1.2 Purpose

The purpose of this Standard is to equip design professionals, data center operators, and non-technical managers with an objective and effective means for identifying the anticipated performance of different data center site infrastructure design topologies.

1.3 References

American Society of Heating, Refrigerating, and Air-Conditioning Engineers, *ASHRAE Handbook – Fundamentals* (Latest Version).

Institute *Fault Tolerant Power Compliance Specification, Version 2.0.*

1.4 Related Publications

Accredited Tier Designer Technical Paper Series

Further information can be found at www.uptimeinstitute.com/resources.

2. Site Infrastructure Tier Standards

2.1 Tier I: Basic Site Infrastructure

2.1.1 The fundamental requirement:

a) A Tier I basic data center has non-redundant capacity components and a single, non-redundant distribution path serving the critical environment. Tier I infrastructure includes: a dedicated space for IT Systems; a UPS to filter power spikes, sags, and momentary outages; dedicated cooling equipment; and an engine generator to protect IT functions from extended power outages.

b) Twelve hours of on-site fuel storage for engine generator(s).

2.1.2 The performance confirmation tests:

a) There is sufficient capacity to meet the needs of the site.

b) Planned work will require most or all of the site infrastructure systems to be shut down affecting critical environment, systems, and end users.

2.1.3 The operational impacts:

a) The site is susceptible to disruption from both planned and unplanned activities. Operation (Human) errors of site infrastructure components will cause a data center disruption.

b) An unplanned outage or failure of any capacity system, capacity component, or distribution element will impact the critical environment.

c) The site infrastructure must be completely shut down on an annual basis to safely perform necessary preventive maintenance and repair work. Urgent situations may require more frequent shutdowns. Failure to regularly perform maintenance significantly increases the risk of unplanned disruption as well as the severity of the consequential failure.

2.2 Tier II: Redundant Site Infrastructure Capacity Components

2.2.1 The fundamental requirement:

a) A Tier II data center has redundant capacity components and a single, non-redundant distribution path serving the critical environment. The redundant components are extra engine generators, UPS modules and energy storage, chillers, heat rejection equipment, pumps, cooling units, and fuel tanks.

b) Twelve hours of on-site fuel storage for 'N' capacity.

2.2.2 The performance confirmation tests:

a) Redundant capacity components can be removed from service on a planned basis without causing any of the critical environment to be shut down.

b) Removing distribution paths from service for maintenance or other activity requires shutdown of critical environment.

c) There is sufficient permanently installed capacity to meet the needs of the site when redundant components are removed from service for any reason.

2.2.3 The operational impacts:

a) The site is susceptible to disruption from both planned activities and unplanned events. Operation (Human) errors of site infrastructure components may cause a data center disruption.

b) An unplanned capacity component failure may impact the critical environment. An unplanned outage or failure of any capacity system or distribution element will impact the critical environment.

c) The site infrastructure must be completely shut down on an annual basis to safely perform preventive maintenance and repair work. Urgent situations may require more frequent shutdowns. Failure to regularly perform maintenance significantly increases the risk of unplanned disruption as well as the severity of the consequential failure.

2.3 Tier III: Concurrently Maintainable Site Infrastructure

2.3.1 The fundamental requirements:

a) A Concurrently Maintainable data center has redundant capacity components and multiple independent distribution paths serving the critical environment. Only one distribution path is required to serve the critical environment at any time.

b) All IT equipment is dual powered as defined by the Institute's *Fault Tolerant Power Compliance Specification, Version 2.0* and installed properly to be compatible with the topology of the site's architecture. Transfer devices, such as point-of-use switches, must be incorporated for critical environment that does not meet this specification.

c) Twelve hours of on-site fuel storage for 'N' capacity.

2.3.2 The performance confirmation tests:

a) ***Each and every*** capacity component and element in the distribution paths can be removed from service on a planned basis without impacting any of the critical environment.

b) There is sufficient permanently installed capacity to meet the needs of the site when redundant components are removed from service for any reason.

2.3.3 The operational impacts:

a) The site is susceptible to disruption from unplanned activities. Operation errors of site infrastructure components may cause a computer disruption.

b) An unplanned outage or failure of any capacity system will impact the critical environment.

c) An unplanned outage or failure of a capacity component or distribution element may impact the critical environment.

d) Planned site infrastructure maintenance can be performed by using the redundant capacity components and distribution paths to safely work on the remaining equipment.

e) During maintenance activities, the risk of disruption may be elevated. (This maintenance condition does not defeat the Tier rating achieved in normal operations.)

2.4 Tier IV: Fault Tolerant Site Infrastructure

2.4.1 The fundamental requirements:

a) A Fault Tolerant data center has multiple, independent, physically isolated systems that provide redundant capacity components and multiple, independent, diverse, active distribution paths simultaneously serving the critical environment. The redundant capacity components and diverse distribution paths shall be configured such that 'N' capacity is providing power and cooling to the critical environment after any infrastructure failure.

b) All IT equipment is dual powered as defined by the Institute's *Fault Tolerant Power Compliance Specification, Version 2.0* and installed properly to be compatible with the topology of the site's architecture. Transfer devices, such as point-of-use switches, must be incorporated for critical environment that does not meet this specification.

c) Complementary systems and distribution paths must be physically isolated from one another (compartmentalized) to prevent any single event from simultaneously impacting both systems or distribution paths.

d) Continuous Cooling is required.

e) Twelve hours of on-site fuel storage for 'N' capacity.

2.4.2 The performance confirmation tests:

a) A single failure of any capacity system, capacity component, or distribution element will not impact the critical environment.

b) The infrastructure controls system demonstrates autonomous response to a failure while sustaining the critical environment.

c) ***Each and every*** capacity component and element in the distribution paths can be removed from service on a planned basis without impacting any of the critical environment.

d) There is sufficient capacity to meet the needs of the site when redundant components or distribution paths are removed from service for any reason.

2.4.3 The operational impacts:

a) The site is not susceptible to disruption from a single unplanned event.

b) The site is not susceptible to disruption from any planned work activities.

c) The site infrastructure maintenance can be performed by using the redundant capacity components and distribution paths to safely work on the remaining equipment.

d) During maintenance activity where redundant capacity components or a distribution path shut down, the critical environment is exposed to an increased risk of disruption in the event a failure occurs on the remaining path. This maintenance configuration does not defeat the Tier rating achieved in normal operations.

e) Operation of the fire alarm, fire suppression, or the emergency power off (EPO) feature may cause a data center disruption.

2.5 Engine-Generator Systems

Engine-generator systems are considered the primary power source for the data center. The local power utility is an economic alternative. Disruptions to the utility power are not considered a failure, but rather an expected operational condition for which the site must be prepared. Accordingly, engine generators must automatically start and assume load upon loss of utility.

2.5.1 Site on Engine-Generator Power

A Tier III or IV engine-generator system, along with its power paths and other supporting elements, shall meet the Concurrently Maintainable and/or Fault Tolerant performance confirmation tests while they are carrying the site on engine-generator power.

2.5.2 Manufactures' Runtime Limitation

Engine generators for Tier III and IV sites shall not have a limitation on consecutive hours of operation when loaded to 'N' demand. Engine generators that have a limit on consecutive hours of operation at 'N' demand are appropriate for Tier I or II.

2.5.3 Regulatory Runtime Limitation

Engine-generator systems often have an annual regulatory limit on operating hours driven by emissions. These environmental limits do not impact the consecutive hours of operation constraint established in this section.

2.6 Ambient Temperature Design Points

The effective capacity for data center facilities infrastructure equipment shall be determined at the peak demand condition based on the climatological region and steady state operating set points for the data center. All manufactures' equipment capacities shall be adjusted to reflect the extreme observed temperatures and altitude at which the equipment will operate to support the data center.

2.6.1 Extreme Annual Design Conditions

The capacity of all equipment that rejects heat to the atmosphere shall be determined at the Extreme Annual Design Conditions that best represents the data center location in the most recent edition of the *ASHRAE Handbook – Fundamentals*. (Each ASHRAE Handbook is revised and published every 4 years.) The design Wet Bulb (WB) temperature shall be the listed Extreme Max WB value and the design Dry Bulb (DB) temperature for design shall be the "N=20 years" value.

2.6.2 Computer Room Set points

The capacity for computer room cooling equipment shall be determined at the return air temperature, and relative humidity established by the owner for steady state data center operations.

2.7 Communications Routing

Conveyance for fiber or communications connections from off site to data center communication demarcation must be in accordance with Concurrently Maintainable requirements for Tier III and Fault Tolerant, Compartmentalized requirements for Tier IV.

2.8 Makeup Water

On-site, backup makeup water storage is required for Tier III and Tier IV sites using evaporative cooling. Accordingly, the makeup water system must also be Concurrently Maintainable and Fault Tolerant as required to the point of delivery for a minimum duration of 12 hours.

2.9 Tier Requirements Summary

A summary of the preceding requirements defining the four distinct Tier classification levels is in Table 1.

Table 1: Tier Requirements Summary

	Tier I	Tier II	Tier III	Tier IV
Active Capacity Components to Support the IT Load	N	N+1	N+1	N After any Failure
Distribution Paths	1	1	1 Active and 1 Alternate	2 Simultaneously Active
Concurrently Maintainable	No	No	Yes	Yes
Fault Tolerance	No	No	No	Yes
Compartmentalization	No	No	No	Yes
Continuous Cooling	No	No	No	Yes

3. Commentary for Application of the Tier Standard: Topology

This Commentary is not part of the Data Center Site Infrastructure Tier Standard: Topology. It provides the reader with context for the application of the Standard.

3.1 Outcome-Based Tier Standard

The definitions used in the Institute's Tier Standard are necessarily and intentionally very broad to allow innovation and client manufacture and equipment preferences in achieving the desired level of site infrastructure performance or uptime. The individual Tiers represent categories of site infrastructure topology that address increasingly sophisticated operating concepts, leading to increased site infrastructure availability.

The operational performance outcomes that define the four Tiers of site infrastructure are very straightforward. Many designs that pass a checklist approach will fail an operational performance requirements approach. This means that, in addition to the rigorous application of engineering principles, there is still considerable judgment and flexibility in the design for uptime and how subsystems are integrated to allow for multiple operating modes.

3.2 Impact of Ambient Design Conditions

The sustainable effective capacity of most cooling and power generating equipment is impacted by the actual ambient conditions in which it operates. These components typically require more energy to operate and provide less usable capacity as altitude and ambient air temperatures rise.

A common practice for conventional facilities is to select design values applicable to most but not all anticipated hours of operation of that facility. This results in an economical choice of equipment that meets requirements most of the time. This is not appropriate for data centers that are expected to operate on a 24 x Forever basis.

Using a DB temperature for design that is exceeded 2% of the time results in selection of a component that is undersized 175 hours of the year. Although this may seem to imply that the owner runs an operational risk for a little over one week each year, these hours actually occur incrementally spread over several days. The 2% design value could result in actual conditions exceeding the design parameters of the equipment several hours every afternoon for a 1- to 2-month period. A 0.4% value, considered conservative by many design professionals, still results in equipment performing below requirements approximately 35 hours each year.

Another example concerning ambient conditions arises when selecting heat rejection systems for split system direct expansion cooling system. Many manufactures provide product selection tables based on 95°F/35°C ambient outside conditions. These components will only produce the nominal capacity listed when operating in up to 95°F/35°C outside air. These component capacities must be adjusted downward to provide the required capacity when temperatures exceed 95°F/35°C.

3.3 Restrictions Against Engine-Generator Runtime Limitation (Tier III and Tier IV)

The intent of the restriction against engine-generator runtime limitation is to ensure the engine-generator plant is capable of supporting the site load on a continuous basis. Tier topology requires that the load capacity of engine generators bearing one of the three main ISO 8528-1 ratings (Continuous, Prime, Standby) must be considered differently, based on the specific rating.

a) **Continuous**-rated engine generators can be run for an unlimited number of hours at the rated kW.

b) **Prime**-rated engine generators can be run for a limited number of hours at the rated kW. This capacity does not meet the intent of Section 2.5. As stated in ISO 8528-1, the capacity of a Prime-rated engine generator must be reduced to 70% (derated) to operate on an unlimited basis. Some manufactures state a different reduced capacity (may be more or less than 70%) at which the engine generator can operate on an unlimited basis either in the product specification, or by separate letter. The manufactures' certification of capacity at an unlimited duration will be used to determine compliance with Tier requirements.

c) **Standby** engine generators are, by definition, held to an annual run-hour limitation. This limitation does not meet the intent of Section 2.5. Some manufactures state a different, reduced capacity at which the engine generator can operate on an unlimited basis either in the product specification, or by separate letter. The manufactures' certification of capacity at an unlimited duration will be used to determine compliance with Tier requirements.

3.4 Tier Functionality Progression

Owners who select Tier I and Tier II solutions to support current IT technology are typically seeking a solution to short-term requirements. Both Tier I and Tier II are usually tactical solutions, i.e., driven by first-cost and time-to-market more than life-cycle cost and uptime (or availability) requirements. Rigorous uptime requirements and long-term viability usually lead to the strategic solutions found more often in Tier III and Tier IV site infrastructure. Tier III and Tier IV site infrastructure solutions have an effective life beyond the current IT requirement. Strategic site infrastructure solutions enable the owner to make strategic business decisions concerning growth and technology, unconstrained by current site infrastructure topology.

3.4.1 Tier I

Tier I solutions acknowledge the owner's desire for dedicated site infrastructure to support IT systems. Tier I infrastructure provides an improved environment over that of an ordinary office setting and includes: a dedicated space for IT systems; a UPS to filter power spikes, sags, and momentary outages; dedicated cooling equipment not shut down at the end of normal office hours; and an engine generator to protect IT functions from extended power outages.

3.4.2 Tier II

Tier II solutions include redundant critical power and cooling capacity components to provide an increased margin of safety against IT process disruptions due to site infrastructure equipment failures. The redundant components are typically extra UPS modules, chillers, heat rejection equipment, pumps, cooling units, and engine generators. A malfunction or normal maintenance will result in loss of a capacity component.

3.4.3 Tier III

Tier III site infrastructure adds the concept of Concurrent Maintenance beyond what is available in Tier I and Tier II solutions. Concurrent Maintenance means that ***each and every*** capacity or distribution component necessary to support the IT processing environment can be maintained on a planned basis without impact to the IT environment. The effect on the site infrastructure topology is that a redundant delivery path for power and cooling is added to the redundant critical components of Tier II. Maintenance allows the equipment and distribution paths to be returned to 'like-new' condition on a frequent and regular basis.

Thus, the system will reliably and predictably perform as originally intended. Moreover, the ability to concurrently allow site infrastructure maintenance and IT operation requires that ***each and every*** system or component that supports IT operations must be able to be taken offline for scheduled maintenance without impact to the IT environment. This concept extends to important subsystems such as control systems for the mechanical plant, start systems for engine generators, EPO controls, power sources for cooling equipment and pumps, isolation valves, and others.

3.4.4 Tier IV

Tier IV site infrastructure builds on Tier III, adding the concept of Fault Tolerance to the site infrastructure topology. Similar to the application of Concurrent Maintenance concepts, Fault Tolerance extends to ***each and every*** system or component that supports IT operations. Tier IV considers that any one of these systems or components may fail or experience an unscheduled outage at any time. The Tier IV definition of Fault Tolerance is based on a single component or path failure.

However, the site must be designed and operated to tolerate the cumulative impact of every site infrastructure component, system, and distribution path disrupted by the failure. For example, the failure of a single switchboard will affect every subpanel and equipment component deriving power from the switchboard. A Tier IV facility will tolerate these cumulative impacts without affecting the operation of the computer room.

3.5 Fractional or Incremental Tier Classification

The four Tier Standard Classifications address topology, or configuration, of site infrastructure, rather than a prescriptive list of components to achieve a desired operational outcome. For example, the same number of chillers and UPS modules can be arranged on single power and cooling distribution paths resulting in a Tier II solution (Redundant Components), or on two distribution paths that may result in a Tier III solution (Concurrently Maintainable).

Consistent, across-the-board application of Tier topology concepts for electrical, mechanical, automation, and other subsystems is required for any site to satisfy the Tier standards defining any classification level. Selecting the appropriate topology solution based on the IT availability requirements to sustain well-defined business processes, and the substantial

financial consequences for downtime, provides the best foundation for investment in data center facilities. It is preferable for the owner's focus during the data center design and delivery process to be on the consistent application of the Tier Performance Standard rather than on the details that make up the data center site infrastructure

However, site infrastructure has been occasionally described by others in the industry in terms of fractional Tiers (e.g., Tier 2.5), or incremental Tiers (Tier III +, Enhanced Tier III, or Tier IV-lite). Fractional or incremental descriptions for site infrastructure are not appropriate and are misleading. Including a criteria or an attribute of a higher Tier Classification in the design does not increase the overall Tier Classification. However, deviation from the Tier objective in any subsystem will prevent a site from being Certified at that Tier.

a) A site that has an extra (redundant) UPS module but needs all the installed cooling units running to keep the computer room temperature within limits does not meet the redundancy requirements for Tier II.

b) A switchboard that cannot be shut down without affecting more than the redundant number of secondary chilled water pumps (reducing the available capacity to less than N) is not Concurrently Maintainable and will not be Certified as Tier III.

c) Including a UPS system patterned after a Tier IV system within a site having a Tier II power distribution backbone yields a Tier II Certification.

3.6 Non-Compliance Trends

The most significant deviations from the Tier Standard found in most sites can be summarized as inconsistent solutions. Frequently, a site will have a robust, Fault Tolerant electrical system patterned after a Tier IV solution, but will utilize a Tier II mechanical system that cannot be maintained without interrupting computer room operations. This results in an overall Tier II site rating.

Most often, the mechanical system fails Concurrent Maintenance criteria because of inadequate coordination between the number and location of isolation valves in the chilled water distribution path. Another common oversight is branch circuiting of mechanical components, which results in having to shut down the entire mechanical system to perform electrical maintenance. If more than the redundant number of chillers, towers, or pumps is de-energized for electrical maintenance, computer-room cooling is impacted.

Electrical systems often fail to achieve Tier III or Tier IV criteria due to design choices made in the UPS and the critical power distribution path. UPS configurations that utilize common input and output switchgear are almost always unmaintainable without critical environment outages and will fail the Tier III requirements even after spending many hundreds of thousands of dollars. Topologies that include static transfer switches in the critical power path for single-corded IT devices will likely fail both the Fault Tolerance criteria and the Concurrent Maintenance criteria.

Consistent application of standards is necessary to have an integrated solution for a specific data center. It is clear that the IT organization invests heavily in the features offered by newer critical environment technology. Often, as the electrical and mechanical infrastructures are defined and the facility operations are established, there is a growing degree of inconsistency in the solutions incorporated in a site. An investment in one segment must be met with a similar investment in each of the other segments if any of the elements in the combined solution are to have the desired effect on IT availability. A well-executed data center master plan or strategy should consistently resolve the entire spectrum of IT and facility requirements.

Modifications

This Standard incorporates the 2010 voting results of the Owners Advisory Committee. The engine-generator fuel storage requirements is effective 1 May 2010.

The changes incorporated are a result of the 2012 discussion and voting by the Owners Advisory Committee. All updates specific to this version are effective 1 August 2012.

About the Uptime Institute

Uptime Institute is an unbiased, third-party data center research, education, and consulting organization focused on improving data center performance and efficiency through collaboration and innovation. The Uptime Institute serves all shareholders of the data center industry, including enterprise and third-party operators, manufacturers, providers, and engineers. This collaborative approach, complemented with the Uptime Institute's capability to recognize trends on a global basis and to interface directly with owners, results in solutions and innovations freed from regional constraints for the benefit of the worldwide data center industry.

Questions?
info@uptimeinstitute.com
+1 206.706.4149

Uptime Institute, LLC
20 West 37th Street, 6th Floor, New York, NY 10018
+1 206.706.4149 · Fax: +1 206.706.3083
http://uptimeinstitute.com · http://uptimeinstitute.com/professional-services

Physical Security Guide
Lead Agency Publication G13-01

Secure Storage Rooms (SSR)

This Guide replaces all previous versions of G1-029

Rev. 1.0 (Original)

Suggestions or comments regarding this guide should be directed to the
RCMP Departmental Security Branch / Physical Security Section
1426 St. Joseph Blvd., Ottawa ON K1A 0R2

Questions may also be emailed to: Physec-secmat@rcmp-grc.gc.ca

This publication is UNCLASSIFIED (For Official Use Only).
It may be provided to contractors, consultants and designers on an as-needed basis.

Contents

Figures

Definitions

Authority Having Jurisdiction – Normally the local city, municipality or county building inspector. For Canadian Forces bases the Authority Having Jurisdiction will be the Canadian Forces Fire Marshall.

Attack Side – The side of the door or wall that is exposed to the adversary.

Base-line Threat – Threat(s) that are common to government departments in Canada under normal security conditions, as specified in the *Operational Security Standard on Physical Security*.

Day Door – A door to a secure room or vault with a primary lock which when unlocked in the morning by the person responsible is still secured by a secondary lock (usually electronic access control) which can be opened (until the primary lock is re-locked) by authorized assistants.

Design-Basis Threat (DBT) – The threat(s) which the specific protection measure (equipment, procedure or policy) is designed to mitigate. Unless specified otherwise, RCMP protective designs and guides are meant to mitigate a DBT based upon the Base-line Threat.

Compromise - The unauthorized access to, disclosure, destruction, removal, modification, use or interruption of assets or information.

Hinge Pair – Industry practice is to specify hinges by pairs. For example, doors with 3 hinges are specified as "1½ pair".

Maximum Security Pin –A hinge pin that has been fixed after insertion by welding, pinning, or other permanent means to prevent hinge pin removal without the use of special tools. Set screws are not permitted. Affords greater security than a Non-Removable Pin. (ref.: ANSI 156.1 (2006)).

Non-Removable Pin – A hinge pin secured by a set screw or other equivalent means (ref.: ANSI 156.1 (2006)).

Open Shelf Storage – storage other than in approved security containers and safes. Open shelf storage includes storage where records are kept in containers or commercial fire and/or water resistant containers.

Safety Stud –A projecting member on one surface of a full mortise leaf that engages a hole in the opposite leaf when the door is closed. (ref.: ANSI 156.1 (2006))

Security Container – a totally enclosed container or specially designed room functioning as a storage container (e.g.: Secure Storage Room).

Secure Room (SR) – Term used to denote a room constructed to specifications of the RCMP Guide G1-029. Although not an RCMP-endorsed practice, these rooms were commonly

constructed to create security zones, secure working rooms (or suites), as well as for secure storage (the original intended application).

Secure Storage Room (SSR) – the formal term and abbreviation used to identify a room which is designed to the specifications of the RCMP Guide G13-01.

Note: The term "Secure Storage Room" does not automatically replace the term "Secure Room" (level 1 or 2). Existing Secure Rooms should only be referred to as Secure Storage Rooms (SSRs) if they are actually being used in a manner consistent with this guide.

Threat and Risk Assessment (TRA) – a consideration of the assets and the threats to those assets in consideration of the sum of the security measures in place or anticipated.
The RCMP and CSEC have jointly developed and promote the use of a formal procedure, checklists, valuation tables and associated training for conducting a TRA in the Federal Government called the Harmonized Threat and Risk Assessment (HTRA).

Vibration Detector – a system of one or more sensors to detect vibrations created by impact and powered cutting tools. Approved systems have a sensitivity / detection algorithm to ensure that ambient and incidental noises or vibrations due to normal activity will not initiate false alarms.

Zones – Defined in Reference B.

Abbreviations

AHJ – Authority Having Jurisdiction.
CCVE – Closed Circuit Video Equipment
Ga – Sheet metal gauge indicating the standard thickness of the sheet metal.
IDS – Intrusion Detection System
SEG – Security Equipment Guide
SCIF – Secure Compartmented Information Facility
SR – Secure Room (+ suffix indicating Secure Room "Type" as per earlier versions of G1-029)
SOR – Statement of Requirements
SSR – Secure Storage Room
TRA – Threat and Risk Assessment
OD – outside diameter
oc – on centre
Ø – bar diameter

References

A. Policy on Government Security
http://publiservice.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578&section=text#cha5

B. Operational Security Standard on Physical Security
http://publiservice.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12329

C. G1-001 RCMP Security Equipment Guide (SEG)
http://www.rcmp-grc.gc.ca/physec-secmat/res-lim/pubs/seg/html/home_e.htm

D. HRSDC Fire Commissioner: Standard for Records Storage
http://www.hrsdc.gc.ca/eng/labour/fire_protection/policies_standards/commissioner/index.shtml

E. HRSDC Fire Commissioner Technical Interpretation: Door and Door Release Hardware with One Release Operation
http://www.hrsdc.gc.ca/eng/labour/fire_protection/policies_standards/interpretations/2008_006.shtml

F. Lock-Up Requirements for Protected A and Protected B Information (published under the "Storage" section of the RCMP Security Equipment Guide.
http://www.rcmp-grc.gc.ca/physec-secmat/res-lim/pubs/seg/html/page_0072_e.htm

Referenced Commercial Standards

These standards are available for purchase from their respective standards associations, or from standards vendors such as IHS Standards (http://global.ihs.com) , the ANSI Store (http://webstore.ansi.org) or Techstreet (http://www.techstreet.com)

ANSI/ BHMA A156.4: *Door Controls-Closers*
American National Standards Institute (http://www.ansi.org/)

ANSI/BHMA A156.1: *Butts and Hinges*
American National Standards Institute/ Builders Hardware Manufacturers Association

ASTM A627-03: *Standard Test Methods for Tool-Resisting Steel Bars, Flats, and Shapes for Detention and Correctional facilities* (http://www.astm.org)

ASTM F1267-07: *Standard Specification for Metal Expanded Steel*
American Society for Testing and Materials

CAN/CGSB-1.60: *Interior Alkyd Gloss Enamel Paint*
Canadian General Standards Board (http://www.tpsgc-pwgsc.gc.ca/cgsb/home/index-e.html)

CSDMA 08 11 13: *Recommended Specification for Commercial Steel Door and Frame Products*
Canadian Steel Door Manufacturer's Association (http://www.csdma.org)

EMMA 557-99: *Standard for Expanded Metal, Introduction, Product Selection Considerations, Terminology, Manufacturing Process, Manufacturing Tolerances and Applications.*
Expanded Metal Manufacturers Association (http://www.naamm.org/emma)

HMMA 840-07: *Guide Specification for Installation and Storage of Hollow Metal Door and Frame*

HHMA 810-09 (NAAMM Standard): *Hollow Metal Doors*
Hollow Metal Manufacturers Association (http://www.naamm.org/hmma/)

SSMA : *Product Specifications*
Steel Stud Manufacturers Association (http://www.ssma.com/technical_library.aspx)

PART I (For use by the Department or Agency)

Advances in portable tool technology have changed the nature of *overt force* and *skilled force* attacks. In addition, large-capacity memory devices can now store significant amounts of information and the threat to personal information has greatly increased due to identity theft. **In light of these technological and threat evolutions, it is recommended that a TRA be conducted on all existing Secure Rooms (or similar spaces constructed using previous G1-029 version specifications) to determine if modifications are warranted.**

Significant Changes introduced with the G13-01:

- There is an emphasis on the Secure Storage Room (SSR) as a special type of approved security container (essentially an alternative to using numerous approved security containers) and on its application consistent with that design premise. The name has been changed from Secure Room (SR) to Secure Storage Room (SSR) to further emphasize the design intent.

- In the past, Secure Room levels (1 or 2) were determined essentially by the choice of metal used in the walls. This guide now permits the selection of one or the other based on cost, availability and construction preference.

- Windows and false ceilings are not part of the Secure Storage Room design and are highly discouraged. When they must be used, compensatory measures will be required. The RCMP can provide guidance on a case-by-case basis.

- There is a new emphasis on the early detection of forced entry.

- This guide attempts to optimize the use of commercial-off-the-shelf (COTS) material and components. Widely accepted commercial standards are referenced whenever practical.

How to Use This Guide

This Guide (particularly Part 1) is intended for use by qualified security practitioners and departmental security staff to select appropriate Secure Storage Room features and Intrusion Detection System (IDS) components and develop a Statement of Requirements (SOR) to guide the designer responsible for its design and construction.

Process

Once the SOR is established, appropriately cleared architects, engineers or qualified builders/ designers should be engaged to develop detailed drawings and specifications. These should incorporate the features and components specified in the SOR and ensure the design conforms to overall project requirements (where part of a larger project) and all applicable codes and facility "fit-up" standards. IDS design and installation should ideally be done by departmental security personnel. Departments without alarm and intrusion system sections should engage an independent (without ties to vendors or installers) consultant to assist with developing the IDS

architecture and help manage the contract and procurement process. They can also be helpful with developing commissioning criteria.

The rationale for any component or feature selection (as well as the nature of the asset and the design-basis threat) should only be divulged to the architect, designer and contractor on a need-to-know basis and only if they have the appropriate security clearance. Consideration should be given to classifying the rationale and key security features.

Note: The fact that a SSR may store classified information does not in itself imply the SSR construction details should have the same classification. It does imply the construction details (as well as purpose and name of the SSR) should be adequately protected.

Segregation of details and distribution on a need-to-know basis will often be sufficient.
The architect or designer should be provided with formal guidance / direction on the preparation of drawings for tender or sub-trades to ensure that sensitive information is not inappropriately divulged. For example, the purpose or name of the room should not appear on widely disseminated drawings, specifications or other contract documents. A generic or numeric name should be used. Sub-trades should receive only enough information to perform their work (eg: partial building drawings and system schematics which do not identify adjacent activities or security-related system details). Security requirements should be incorporated into contract documents where feasible to ensure enforceability.

Purpose of the Secure Storage Room

A Secure Storage Room is intended to function as an approved storage container for *open-shelf storage* of a large amount of classified or highly sensitive non-national (Protected) information or assets. A Secure Storage Room is essentially a “security container” and subject to the same zoning requirements.

Unless all mandatory technical and application specifications in this Guide are met, the room does not qualify as an approved Secure Storage Room (SSR) and should not be referred to as an SSR.

- **Fire Protection**

Fire requirements (legislation) ALWAYS supersede security requirements (policy) so good planning and early consultation with the local AHJ is very important to avoid issues which may result in the removal or modification to security features.

Sprinklers are not an integral component of a Secure Storage Room and should not be added inside an SSR unless required by the AHJ. If additional fire protection is required, records can be stored in commercial fire rated containers placed inside the Secure Storage Room. Inert gas fire suppression systems can also be used.

Additional or Type X drywall sheets can be installed to meet code requirements (or as required by the AHJ). If necessary, an appropriately labelled fire door can be used instead of the specified

door. Please note that there are specific requirements for mounting locks and hardware on fire rated doors. Contact the local AHJ for assistance and guidance on fire and safety issues.

Slab–to-Slab

Secure Storage Room walls must be slab-to-slab (from the finished floor to the underside of structural concrete roof or floor) or continue across the ceiling to form a continuous secure enclosure (Secure Ceiling). Where the space above the Secure Ceiling (measured to the underside of the limiting structural component) exceeds 6 inches, the space should be closed and secured or electronically monitored. In rare cases, the floor may also need special treatment. Consult the RCMP for advice.

Design-Basis Threat and Secure Storage Room Design Premise

Secure Storage Rooms primarily protect against surreptitious attacks but also detect and delay forced entry. The SSR is designed for location in a Security Zone or High Security Zone in a federal government building (or CISD-approved equivalent in contractor facilities) in urban centres. SSR constructed in remote locations may require additional safeguards.

A Vulnerability Assessment should be conducted to determine if a potential adversary can access the perimeter (or any space above or below) of the SRR undetected and unobserved for long periods of time. If so, additional measures are required to limit access or *actively* monitor activity in the perimeter areas.

Floors and ceilings are assumed to be constructed of highly intrusion-resistant materials such as structural concrete, reinforced concrete block or concrete on steel (roofs and floors). Wood or steel assemblies should be steel-strengthened and vibration-monitored the same as the walls.

Vestibules

A vestibule was included with the original Secure Room design for two purposes: to limit the swinging motion of hand tools and to provide better sound isolation at the door. With respect to the first objective, the most viable forced entry threat to the SSR door and hardware is now from powered portable tools and a vestibule does little to reduce it. In fact, a vestibule now becomes a possible space for an adversary to hide while attacking the door (or the wall around it). The vestibule is also not needed to enhance sound isolation at the door when the SSR is used as intended – as a records storage room.

Therefore, exterior vestibules are not required (though still permitted) for construction of a SSR. Any vestibule that is built should be constructed so as to permit observation of activities within it (eg: glazed walls or door).

A “day door” function is facilitated by use of SEG-listed locks which provide this function where departmental policy accepts the practice. To be approved for this function, the electronic access controls must work only when the mechanical lock is “open” (locking the mechanical lock must mechanically disengage the electronics so that attacks by compromising the access controls are not possible).

Well-defined and enforced operating procedures are necessary when using “day doors”. Users must not be permitted to use the electronic locking mechanism in place of the mechanical lock for extended periods (especially overnight and weekends).

Intrusion Detection Systems (IDS)

While the sheet steel on the walls provides some force resistance, its main use is to transmit vibrations from force attacks to vibration sensors. The RCMP has tested and approved a vibration detector for SSR walls which is listed in the SEG. Detection systems (e.g. motion sensors) located inside the Secure Storage Room may also be employed, although they do not detect the adversary until he/she has already gained entry, thereby reducing the available response time.

The selection table suggests what type of detection system should be used for various situations. In all cases, the alarm systems must generate reliable, timely and appropriate response.

Plumbing and Electrical Pass-through Construction

Minimize plumbing and electrical pass-throughs in SSR walls where possible. Do not locate pass-throughs in the Critical Attack Area. Where pass-throughs are required, frame openings within 1 inch (25mm) of the pipe/conduit and secure to the stud framing at minimum two places. Extend the wall protection material to within ¾” (20 mm) of the edge of the opening. Extend gypsum wall board to the edge of the pipe or conduit. Seal all gaps with fire rated or acoustic sealant. Recommended product standard: ASTM E 814 (UL 1479) or CAN/ULC S115, or as required by the AHJ.

Where necessary to accommodate pipe or conduit movement or expansion, pipes and conduit may be enclosed in a close-fitting sheet metal sleeve and the sleeve mechanically fastened to the stud framing at two places (minimum). Clearance between the sleeve and pipe or conduit should be kept to a minimum and not exceed ¼”.

Steel bars should be installed to delay access of a person through a duct with a cross-sectional area greater than 96 square inches and a smallest dimension greater than 6”. They may be omitted if a TRA determines that unauthorized entry through these ducts is not a threat.
Note that Man Bars do not prevent the introduction of deleterious material (e.g. water, toxic fumes). If a TRA identifies such threats as viable, all ducts and openings may require additional mitigation measures (e.g.: filters or dampers). Contact the RCMP for advice.

Door Locks

A code-compliant (single motion, single action) door lock that accepts approved combination locks has been approved and is listed in the SEG.

Two-Person Integrity

Some SEG-listed electronic combination locks permit the application of a two-person integrity (both persons must dial the lock open) policy. This is one of the most effective security measures that can be applied to sensitive information storage.

Screws

Screws (including “security screws”) are not approved for attaching wall protection material (sheet or mesh) to metal studs.

Screws are permitted for attaching anti-spread and cross-bracing to metal studs. They may also be used (with washers) to attach steel sheets to wood joists or wood studs.

Standard drywall screws are approved for attaching gypsum wall board to metal or wood studs.

Statement of Requirements

Where the department (client) is not also the designer, a Statement of Requirements (SOR) should be developed to tell the designer exactly what is required and to identify selected construction options from those presented in the General Specifications in Part II.

The SOR and all documentation leading to the selection of SSR specifics should be considered sensitive and treated accordingly.

Do not tell the designer why a selection has been made unless the designer has a need to know.

Advice and Guidance

Royal Canadian Mounted Police
Departmental Security Branch
Physical Security Section
1426 St. Joseph Boulevard
Ottawa, Ontario K1A 0R2
Email: Sec-Equip@rcmp-grc.gc.ca

Table 1 – Security Recommendations

Sensitivity	Security Measures
Protected A **Protected B**	**SSR not required.** "Lock-Up" the information **(**see reference F) A storage room constructed in close conformance to this guide will greatly exceed the minimum "lock up" physical security requirements. The following are recommended alternatives for SSR for storage of Protected A/B: - ½" plywood instead of sheet or mesh steel - UL 634 door contact and IDS (where recommended in TRA) - ANSI 156.13 Grade 1 mortise lock with UL 437 High Security (keyed) Cylinder
Protected C	**Non-Life Threatening** - **Locate SSR in Security Zone**. - Vibration detection on walls (and Secure Ceiling if applicable). - IDS inside the SSR. - Consider additional compartmentalization [1] - SEG-listed combination locks approved for Top Secret / Protected C, or SEG-listed locks approved for Secret (if supported by the DSO) **Life Threatening** - **Locate SSR in High Security Zone** (exterior constructed as recommended in TRA) - Vibration detection on walls (and ceiling or floor if applicable). - Motion detection (or other IDS) inside the SSR. - Additional compartmentalization [1,2]. -Two-person authentication[3] - Formal TRA to ensure the adequacy of measures. - SEG-listed combination locks approved for Top Secret / Protected C.
Confidential	**Locate SSR in Security Zone** - Motion detection (or other IDS) inside the SSR. - Keyed mortise locks. ANSI/BHMA 156.13 Grade 1 or select from SEG. - High Security Cylinders: UL 437, ANSI 156.30 Level "A" or ANSI 156.5 Grade 1A.[4] - Commercial electronic keypad locks are permitted but 'scramble' keypads are preferred. Specify ANSI/BHMA A156.30 level "B"(minimum) or UL 1034.
Secret	**Locate SSR in Security or High Security Zone** - Vibration detection on walls (and floors or ceiling if applicable). - Motion detection (or other IDS) inside the SSR. - SEG-listed combination lock.
Top Secret	**Locate SSR in High Security Zone** - Vibration detection on walls (and Secure Ceiling if applicable). - Motion detection (or other IDS) inside the SSR. - Consider additional compartmentalization for need-to-know[2]. - Consider two person authentication[3] - SEG-listed combination locks approved for Top Secret. - Formal TRA to ensure the adequacy of all storage, alarm and response measures.

Table Notes

1. UL 687 labelled Burglar Resistant safes provide significant additional force resistance (as well as compartmentalization for need-to-know segregation). Although the Secure Storage Room provides early detection and some delay, the safe's resistance time should closely correspond to the assured response time for an appropriate response.

2. Additional compartmentalization is recommended where the need-to-access principle is still a concern (see Reference B paragraph 7.6.7). Information can be compartmentalized by using commercial locking containers/ cabinets. UL 437 high security keyed locks are recommended.

3. Procedural and / or technological mitigation measures should also be considered.

4. Consider the use of High Security cylinders with "chip technology" (e.g. CLIQ ™) for audit purposes (only).

General Notes:

A) Where a TRA determines that a particular threat is well-mitigated by other aspects of security the DSO may decide that one or more of the recommended measures are not required.

B) The Communications Security Establishment of Canada (CSEC) requires certain equipment to be placed in a Secure Room (previously the SR-2). Additional security features such as emanations protection may be required, but the RCMP can only advise on the construction of a Secure Storage Room as designed for records storage. Contact CSEC Client Services: comsecclientservices@cse-cst.gc.ca

Frequently Asked Questions

Q1: Why does Protected "C" in a Secure Storage Room still require a safe?

A1: The nature of the threat to Classified information differs significantly from the threat to Protected "C" (especially Life Threatening) information. Secure Storage Rooms are an alternative to approved security containers and must provide at least the same protection. Protected "C" (especially Life Threatening) is considered susceptible to sustained force attacks by a motivated adversary and thus needs significant force resistance. This can best be assured by using UL 687 Burglar Resistant safes with at least a 1 hour rating for the additional compartmentalization. Safes also provide additional compartmentalization for need-to-know.

Q2: How do the Secure Storage Room requirements relate to those for a Secure Server Room as specified in G1-031?

A2: The functions of the rooms are different. Secure Storage Rooms are designed for the storage of records. They are not intended for the processing of information (or for occupancy). Servers are vulnerable to different threats than stored records, and server rooms generally have extensive electrical, air conditioning, vents and ducts, and other systems in the room (and through the walls).

Q3: The Operational Security Standard on Physical Security says Confidential information can be stored in an Operations Zone. Why does Table 1 recommend that the Secure Storage Room for Confidential information be in a Security Zone?

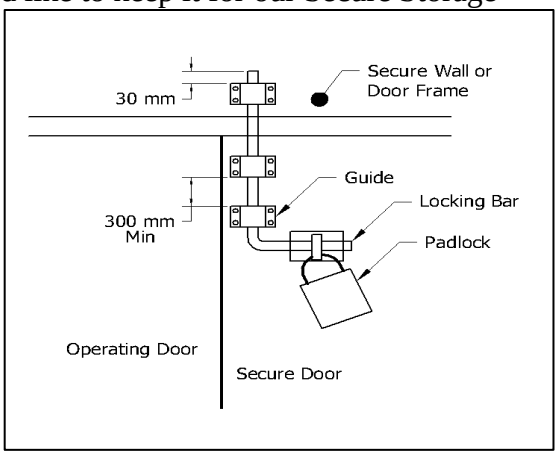
A3: The Secure Storage Room should be in a Security Zone because of the elevated risks associated with storing large amounts of information on open shelves. The "periodic monitoring" requirement for an Operations Zone does not provide assurance that an adversary will not benefit from long periods of unmonitored activity. The concern is that without effective 24/7 monitoring, an adversary could gain access and operate without detection for an extended period of time. Access might be by insecure ceiling spaces or by un-alarmed/ un-monitored exit doors or elevators. If a TRA reveals that the Operations Zone is sufficiently secure that unauthorized access is highly improbable, then the DSO may permit a Secure Storage Room to be located there.

Q4: The space assigned to us for a Secure Storage Room is adjacent to a public space or non-departmental occupant. What should we do?

A4: A Secure Storage Room should never be placed against exterior walls other than those made of reinforced concrete or reinforced concrete blocks (all voids filled). Secure Storage Rooms can normally be placed adjacent to subterranean (basement) walls and walls at least 3 storeys above an accessible surface (ground or roof) without additional safeguards.

If the location cannot readily be changed and the wall construction is reinforced concrete, reinforced concrete block or similar construction, construct a Secure Storage Room wall against the existing wall. To facilitate erection, place the steel mesh on the inside and do not cover it or block completely with shelving. The steel mesh enables users to readily verify that the existing wall behind the mesh is intact. Where feasible, provide early detection or monitoring of the exterior. Consider fences or other barriers. Where early detection is not feasible, review the response time to the intrusion alarm inside to ensure it is adequate.

Q5: We have an existing double steel door and would like to keep it for our Secure Storage Room as it makes it easier to use a forklift. Can we use it?



A5: If the door and frame meet the basic construction requirements of this Guide you may be able to secure one of the doors to provide satisfactory security when closed and secured. One way to do this would be to install heavy duty locking bars at the top and bottom that can be secured with padlocks (to ensure users do not open them and leave them open). The bars should have a diameter of at least 30mm and be connected to the door with two guides that are welded or riveted to the door and spaced at least 300mm apart. The bars must project at least 30mm into a pocket or guide welded or riveted to the frame or secure wall. The bars should have a design that prevents unlocking when the padlock is attached.

This approach requires strict adherence to policy and procedure and should be used with discretion. A custodian should be appointed to hold the keys to the padlocks and be responsible for ensuring the secondary door is secured.

Q6: Are there any restrictions on wall switches or outlets on Secure Storage Room walls?

A6: The Secure Storage Room walls were tested without holes or penetrations. Surface mounted fixtures should be used where possible. Where a fixture must be set into the wall, it should be located as far as possible from the door. The fixture box must be steel and welded or riveted to the steel wall sheathing. All cables and wires should be encased in steel/EMT conduit.

Through penetrations are to be avoided. Where penetrations must be made on both sides of the wall, they should be offset at least 300mm from each other.

Q7: The G13-01 uses mandatory language with words like “required” but isn’t it a ‘guide’?

A7: As Lead Agency, the RCMP is delegated the authority to design, test, evaluate and approve security equipment. Each department or agency has the authority to decide if it will use RCMP approved equipment or designs – either as approved or modified in some way. To be approved, a Secure Storage Room must be constructed to the RCMP design specifications. If all RCMP specifications are not met, it is not an RCMP approved Secure Storage Room and should not be referred to as a Secure Storage Room (SSR).

Q8: What if the AHJ requires the SSR to have two means of egress?

A8: This should not occur when the room is kept to its original design purpose as a (relatively) small records storage room since the secondary exit is determined by occupancy and floor area. If this situation arises, the second exit door should not have any locking hardware on the outside.

Q9: Can I build an SSR in a wooden building?

A9: The SSR was designed for location in a Security or High Security Zone within a typical government building in an urban environment. For other situations, conduct a TRA taking into consideration the threat, the asset and the sum of all protection measures (e.g.: location on a military base, regular patrols and fast response, etc.). While not explicit in this guide, operational security measures that are sufficient and assured can offset minor gaps in the level of physical protection afforded by wooden floor and ceiling construction. Metal protection material and vibration sensors should be installed on both the floor and ceiling of an SSR constructed in a wooden building – contact the RCMP for additional guidance.

Q10. We are putting in an enforcement unit in a warehouse bay with a main floor and a mezzanine floor that will be open to the main floor. However, there will be enclosed offices on this floor. There are plans for two evidence/secure storage rooms on the main floor underneath the mezzanine floor. The floor will not be slab concrete. What should we do?

A10. Where the roof (mezzanine floor) is made of wood (wood or composite joists with plywood sub-flooring), we recommend that the roof have expanded metal mesh (3/4" - #9F as called for in the wall construction) secured to the underside (secure side) of the roof joists and a vibration detector (sensor) installed in contact with the mesh on the secure side. The sensor mounting plate can be installed adjacent to the roof joist (preferred solution). Cabling for the roof sensor should

be run on the secure side of the SR ceiling (i.e. in surface mounted conduit) to where it joins the other sensor cabling in the common conduit to the alarm control panel.

Q11. Can I install the door lock at a different height to accommodate accessibility requirements?

A11. Ordinarily installing the door lock 44 inches above floor level will accommodate accessibility requirements for all users. If the lock is being installed less than 42 inches above floor level, the anti-spread bracing (between the door frame and adjacent stud – located 48 inches above the floor) should be lowered to within 6 inches of the lock center-line, or additional anti-spread bracing installed 6 inches or less below the lock center-line.

Q12. Can I change the lock height (e.g., to accommodate a handicapped person)?

A12. Yes. If the lock height is shifted more than about 150mm (6”) we recommend also shifting the anti-spread bracing to match.

PART II – SSR Construction Specifications

SSR General Construction and Assembly Specifications

Note: The specifications in this Part should be modified as required and incorporated into the Project Contract Documents by the Designer in accordance with client requirements (ideally outlined in a detailed SSR Statement of Requirements) and overall project and code requirements.

Wall Framing (figure 1)

Extend wall partition framing slab to slab.

Top and Bottom Tracks:
SSMA standard: 1- 5/8" x 6", 18ga (600T162-43); or
Preferred: 2" x 6", 18ga (600T200-43)

Secure top and bottom steel stud track to both slabs at 300mm oc using any expanding (preferably double expanding) mechanical fastener. Non-expanding (e.g. "Tapcon") screws are not acceptable.

Studs:
SSMA standard: 1- 5/8" x 6", 18ga (600S162-43: 33ksi); or
Preferred: 2" x 6", 18ga (600S200-43: 33ksi)

Space studs at 300 mm oc and secure to the top and bottom tracks with welds or rivets (not screws).

Install double (jamb) studs at the door frame opening. Install the door frame as per HMMA 840-07, part 3 A, B, C, D and E (except that screws shall be replaced with steel rivets).

Install anti-spread bracing approximately 48" from the bottom of the wall between the door frame double stud and the adjacent stud on both sides of the frame.

Construct wall corners with double studs.

Notes:

1. Leaving a small gap and using drywall sheets to brace frame sections during wall erections is permitted provided steel sheets on the attack side are continuous over all gaps.
2. Drawings of doubled studs are representative. Connect and orient doubled studs as per standard industry practice.

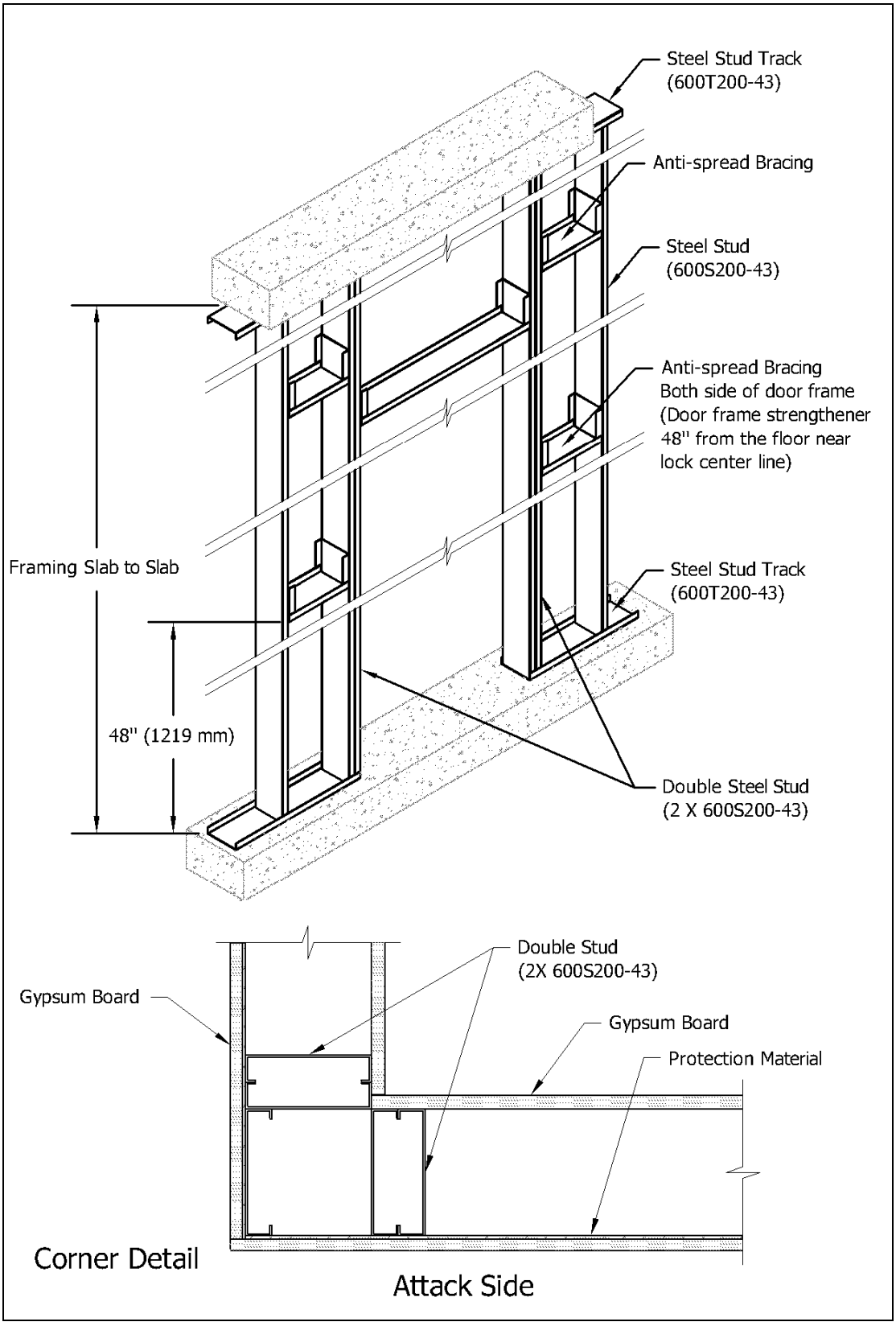


Figure 1: Wall Framing Detail

Wall Protection Material (Figures 2 to 4)

Wall protection material may be one of two options:

Flattened Metal Mesh: To EMMA 557-99. Style ¾-9F: nominal strand thickness of 0.120" (0.108" to 0.132"). Diamond opening of 0.563" x 1.688".
OR
Sheet Steel: 16 Ga, A1008 / A1008M (cold rolled) or A1011/ A1011M (hot rolled) or equivalent.

Mount on the outside (attack side) of the room. Support all edges by anti-spread bracing, studs or corners. Align the sheet edges at every vertical and horizontal seam on the centre line of the steel stud or anti-spread bracing and secure all sheets with welds or rivets.

Note: Screws (including "security screws") are **NOT** acceptable for permanently attaching the protection material (steel or steel mesh). Screws may be used to "tack' the sheets in place pending riveting or welding. Temporary screws do not need to be removed.

Welding (Permitted Method)

Steel mesh (Figure 2): 3mm fillet weld along the strand at 200mm oc

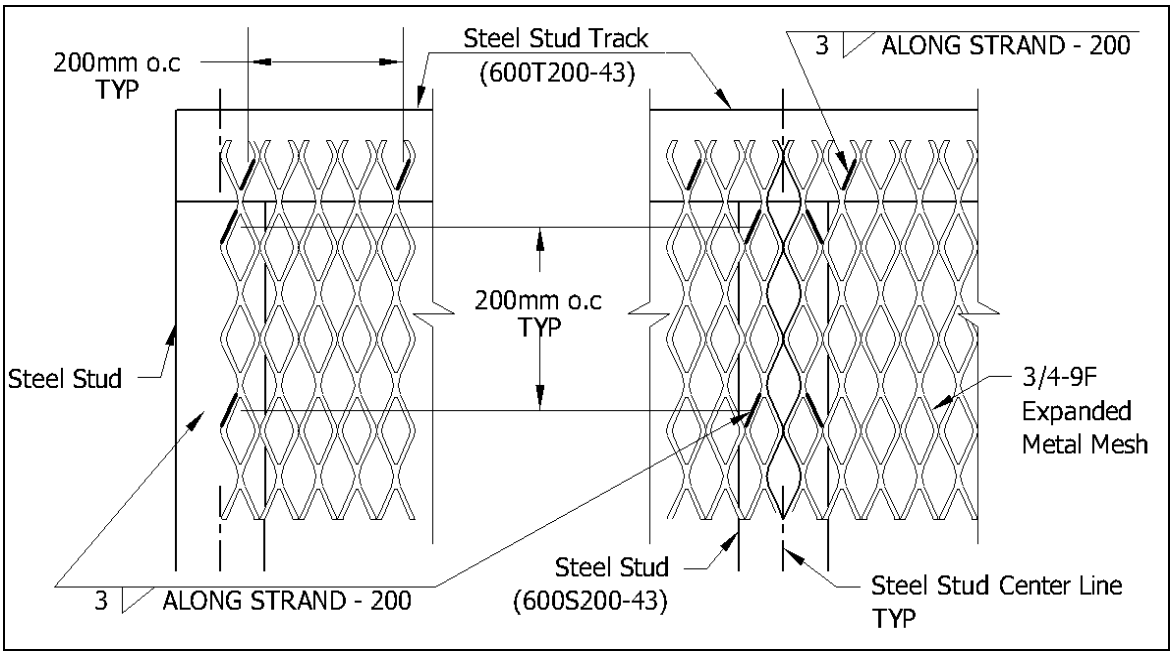


Figure 2: Welding Steel Mesh

Steel Sheet (Figure 3): 1.5mm fillet weld 15mm long at 200mm oc **or**
8mm plug weld at 200mm oc

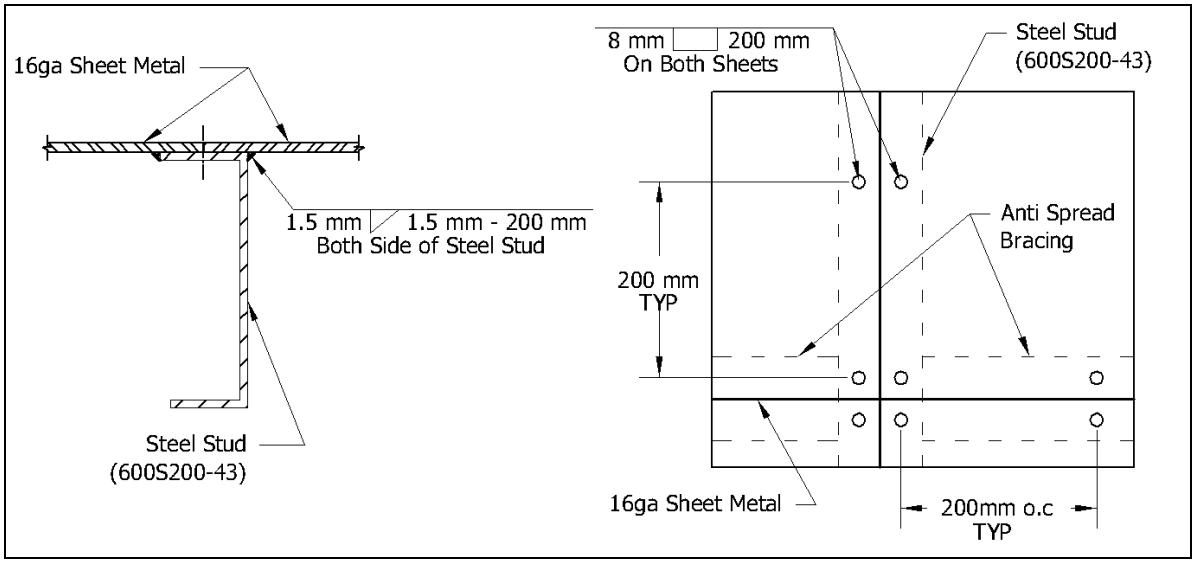


Figure 3: Welding Sheet Steel

Rivets (Preferred Method)

Steel sheet: 3/16" steel rivets at 200mm o.c.
Steel mesh: 3/16" steel rivets and “fender” washer (1 ½ " OD, 3/16’’ ID) at 200mm o.c.

Suggested material:
Rivets: 3/16” steel pop rivet: Speaneur part #301-440
Washers: 1 ½ " OD, 3/16’’ ID “fender” washer: Fastenal part #1133204

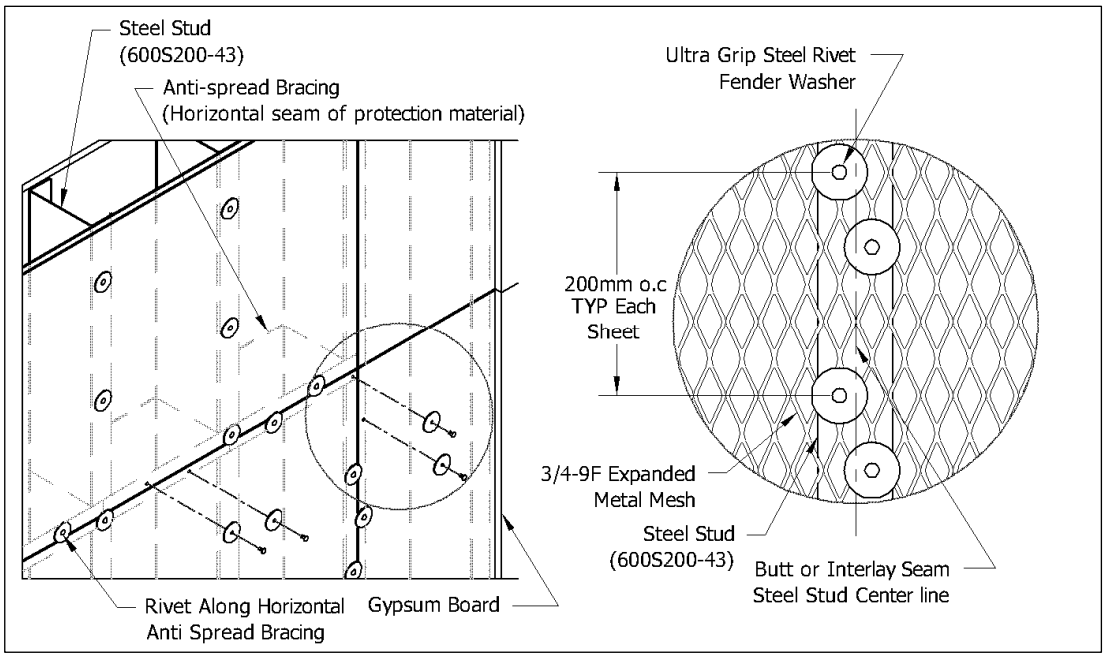


Figure 4: Riveting Sheet or Mesh

Figure 5: Example of Mesh Interlay Seam, Riveted

Critical Attack Area (Figure 6): 16 ga. (1.6 mm) steel sheet, HR Commercial quality, ASTM A366, matte finish, shall extend 1200mm around the door frame on the inside of the secure storage room and be attached as per selected rivet or welding requirements for protection material.

Note: Perforations for services, conduits or ducts are not permitted in the Critical Attack Area.

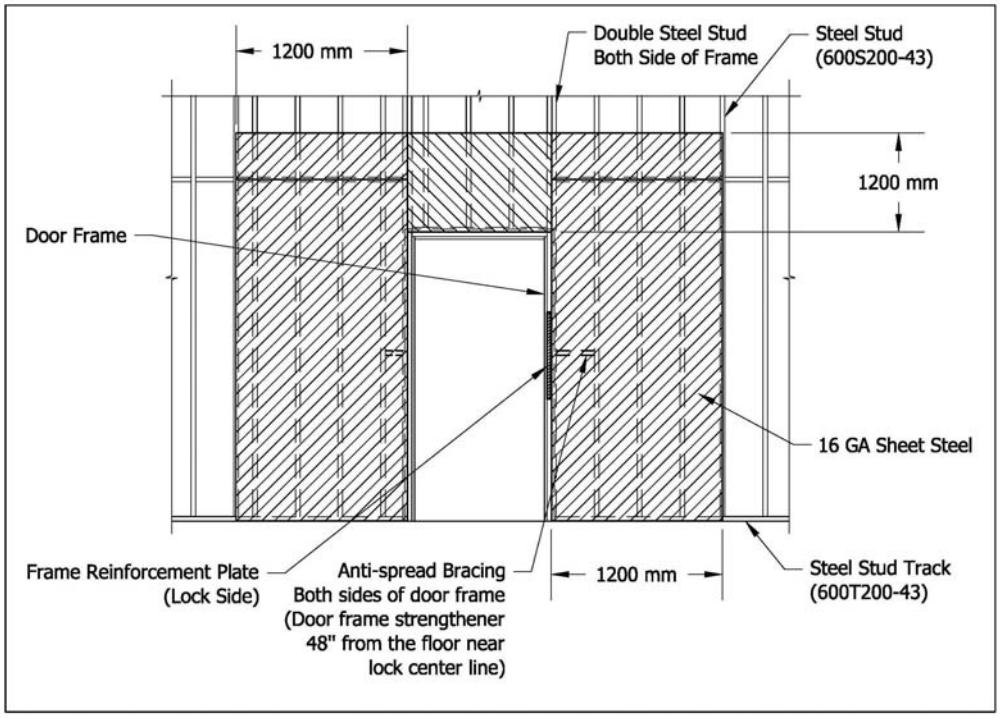


Figure 6: Critical Attack Area Wall Reinforcement

Wall Finishing Details
Install 16mm gypsum wall boards on both sides of the wall (interior is optional).
Standard drywall screws are acceptable for attaching the drywall.

Apply continuous bead of fire-rated acoustic sealing on both sides of the top and bottom tracks. ASTM E814 (UL1479), ASTM E1966 (UL 2079) or CAN/ ULC S115 test standards with a fire/ smoke rating acceptable to the Authority Having Jurisdiction (AHJ).

Paint exterior surface of wall with one coat primer/sealer and one coat of gloss enamel. Primer/sealer must extend above drop ceilings to the bottom of structural ceiling. Paint must be uniform and without blemishes. Joints must not be visible. Custom colors should be considered.

Door, Frame and Hardware

Door and Frame – Commercial Steel Door and frame compliant with section 08-11-13 of CDMA Publication: *Recommended Specification for Commercial Steel Door and Frame Products.*
Door may be specified as fire rated where required.
Doors wider than 900mm (36”) should be avoided. Double doors will require special measures.

Door:

Face Gauge: 16 gauge (1.6 mm) steel
Construction: Laminated core with vertical steel stiffeners at 150mm oc (stiffeners welded or laminated to each face sheet with voids between stiffeners filled with fiberglass or mineral batt type material).
Caps: ‘Flush Closing Channel’ or ‘Flush Channel’ top and bottom.
Ref: NAAMM 810-09 Part 2. A. Figures E and F for edge details.
Edges: all edges and top and bottom caps to be continuously welded and ground smooth.
Door handing: (must be specified as per client requirements).

Frame:

Gauge: 16 gauge (1.6mm) steel
Frame construction: Welded or fully field welded 3-piece “knock-down” (for retrofit applications).
Anchors: “Z” shape steel wall anchors welded to frame.
Reinforcing at latch: as per lock manufacturer recommendations. Lock specifications must be provided to the supplier/manufacturer to provide necessary reinforcing requirements.

Locks: Select according to Table 1.

Hinges: to ANSI/BHMA A156.1 Grade 2 and ANSI A8112 (Steel Material Standard)
Full mortise, five knuckles, ball bearings, standard weight. Three (3) hinges per door (minimum).
Minimum Dimensions: 114mm (4 ½") x 114mm (4 ½") x 3.4mm (0.124") thick.

Hinges mounted with barrels on the attack side ("reverse-hung" or outwards opening) must have non-removable pins (NRP), maximum security pins (MSP) or safety studs/reverse safety studs. Note that these require special ordering instructions.

Suggested products:

- Hager (http://www.hagerco.com) Catalogue item BB1279
- Stanley Architectural Hardware (www.stanleyhardware.com) Catalogue item FBB179
- Mont-Hard (Canada).. Mont-Hard products are carried by Montreal Hinge (www.montrealhinge.com). Catalogue item BB-1079

Door closer: Overhead style ANSI A156.4 Grade 1
Suggested product: Ingersol-Rand LCN 4040 series

Threshold: Aluminum (or other metal) interlocking style with hook strip installed on door. The SSR should qualify for exception from building code "Barrier-free path" requirements when used only to store records. However, where wheelchair accessibility is required, two recommended products are:

- PEMKO (model 114): PEMKO (Toronto) 866-243-9816 (sales), www.PEMKO.com
- Zero International (model 73A): www.Zerointernational.com

Door contacts: UL 634 High Security Switch - level 1 or level 2.

Door installation:
The door is generally installed as regular hung (opening into the Secure Storage Room), but it can be reverse hung (opening out) in exceptional cases.

Frame reinforcement at the lock area: (Figure 7)
Secure a 6.4mm x 25mm x 610mm steel plate inside the frame using tack welds on every edge. Align the centre of the plate with the lock bolt.

For reverse hung doors, install a "Z" type astragal covering the entire lock edge of the door. The astragal should be 14 ga (2 mm) thickness and conform to ASTM A653 or A653M.

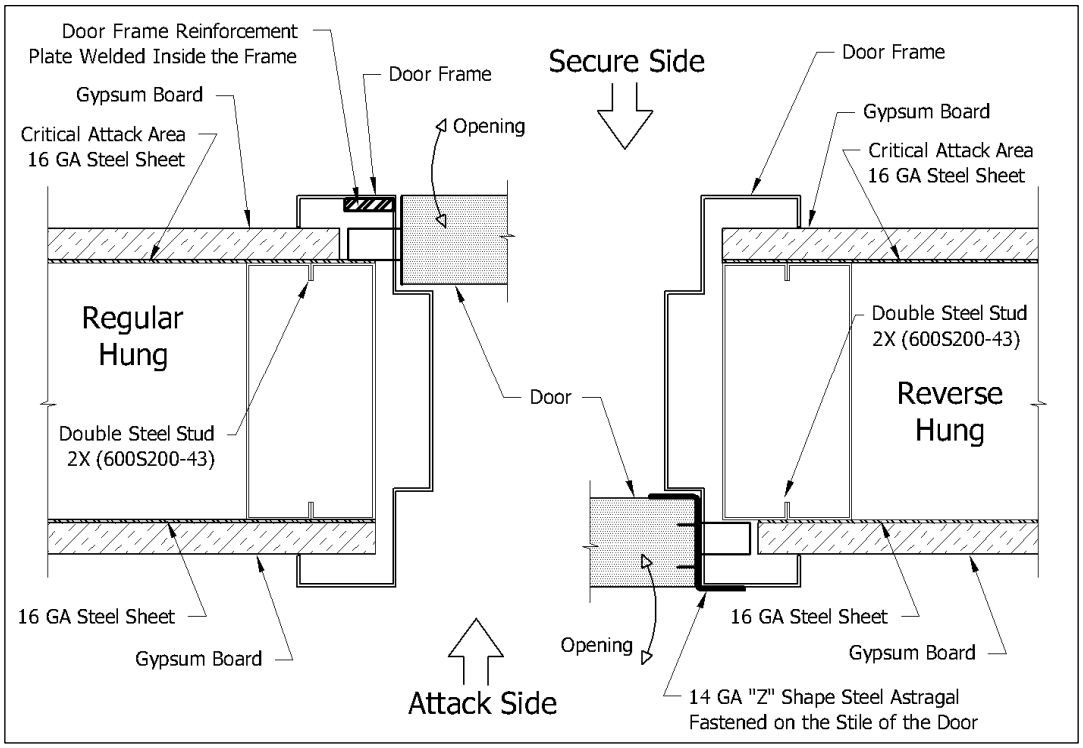


Figure 7: Frame Reinforcement at Door

Ventilation Duct Pass-throughs

Note: Where superior resistance to cutting is required, man bars can be specified as tool-resistant steel (grade 1 or 2) per ASTM A627.

Ceiling mount: (Figure 8)

1. Duct sleeve to be at least the same thickness as duct passing through.
2. The overall dimension of the sleeve must be slightly greater than the duct.
3. Construct frames of 1- 3/8” x 1- 3/8” x 1/8” angle steel welded around duct sleeve (ceiling mount brackets are recommended).
4. Space 3/8” Ø steel bars at 6” oc and weld to the frame.
5. Secure the duct sleeve to the structural ceiling with mechanical fasteners.
6. Cut protection material ¾” max from the edge of the duct opening (3 sides)
7. Apply fire-rated caulking between duct sleeve and finished wall.

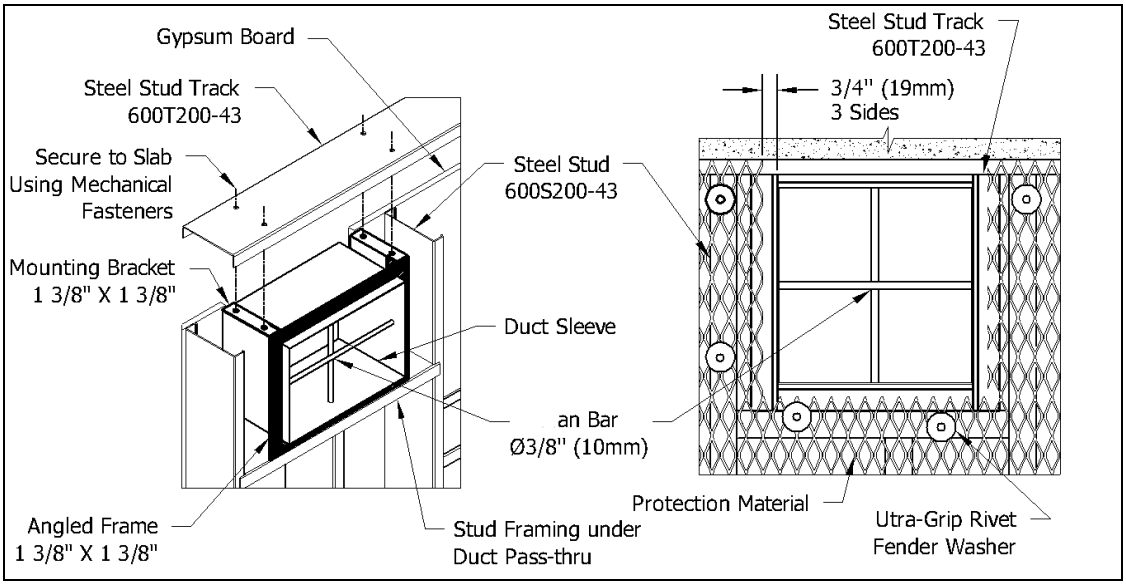


Figure 8: Ceiling Mount Duct Pass-Through

Surface Mount: (Figure 9)

1. Duct sleeve to be at least the same thickness as the duct passing through.
2. The overall dimension of the sleeve must be slightly greater than the duct.
3. Construct frame on each side of the wall of 1- 3/8” x 1- 3/8” x 1/8” angle steel welded around duct sleeve.
4. Space 3/8” dia man bars at 6” oc and weld to the frame.
5. Secure duct sleeve with ¼” dia bolts and hex nuts (inside the room) at 8” oc around the outside duct sleeve. The bolt head shall be on the attack side and be welded in at least three places to the angle frame.
6. Framing around duct sleeve is required.
7. Apply fire-rated caulking between duct sleeve and finished wall.

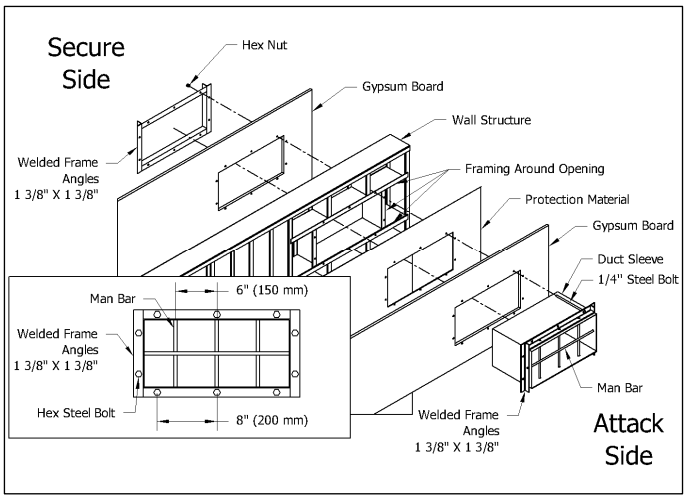


Figure 9: Surface Mount Duct Pass-Through

Physical Security Guide
Lead Agency Publication G13-02

Secure Demising Wall
Lead Agency Guide

Rev 1.0 (Original)

Suggestions or comments regarding this guide should be directed to the
RCMP Departmental Security Branch / Physical Security Section,
1426 St. Joseph Blvd., Ottawa ON K1A 0R2

Questions may also be emailed to: Physec-secmat@rcmp-grc.gc.ca

This publication is UNCLASSIFIED (For Official Use Only).
It may be provided to contractors, consultants and designers on an as-needed basis.

Contents

Figures

Definitions

Authority Having Jurisdiction - Normally the local city, municipality or county building inspector. For Canadian Forces Bases the Authority Having Jurisdiction will be the Canadian Forces Fire Marshall.

Attack Side – The side of the door or wall that is exposed to the adversary.

Base-line Threat –Threats common to government departments in Canada, under normal security conditions, as defined in the *Operational Security Standard on Physical Security*.

Designer – a qualified person (architect, engineer, technologist or other) tasked to develop the specific project design (drawings and specifications) based on the client-generated Statement of Requirements (SOR) and conforming to the overall project and code requirements.

Secure Demising Wall – a force-resistant wall constructed according to RCMP Guide G13-02.

Secure Working Room – a specially designed room, suite of rooms or spaces used for the processing and open shelf storage of classified information.

Statement of Requirements – The client-generated list of project-specific requirements (especially selection of optional alternatives) for the SDW. The SOR should be developed from the advisory information in Part I of this Guide, along with specialist advice as required.

Open Shelf Storage – storage other than in approved security containers and safes. Open shelf storage includes storage where records are kept in containers or commercial fire and/or water resistant containers.

Zones – defined in Reference B.

Abbreviations

dB - decibel
Ga – Sheet metal gauge
SR – Secure Room
SDW – Secure Demising Wall
SSR – Secure Storage Room
SWR – Secure Working Room
SOR – Statement of Requirements
STC – Sound Transmission Classification
TRA – Threat and Risk Assessment
ID – Inside diameter
OD – outside diameter
oc – on centre
Ø - bar diameter

References

A. Policy on Government Security
http://publiservice.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578&section=text#cha5

B. Operational Security Standard on Physical Security
http://publiservice.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12329

Referenced Commercial Standards

The following standards are available for purchase from their respective standards associations, or from standards vendors such as IHS Standards (http://global.ihs.com) , the ANSI Store (http://webstore.ansi.org) or Techstreet (http://www.techstreet.com)

ASTM A627-03: *Standard Test Methods for Tool-Resisting Steel Bars, Flats, and Shapes for Detention and Correctional facilities* http://www.astm.org/

ASTM F1267-07: *Standard Specification for Metal Expanded Steel*
American Society for Testing and Materials http://www.astm.org/

CAN/CGSB-1.60: *Interior Alkyd Gloss Enamel Paint*
Canadian General Standards Board http://www.tpsgc-pwgsc.gc.ca/cgsb/home/index-e.html

EMMA 557-99: *Standard for Expanded Metal, Introduction, Product Selection, Considerations, Terminology, Manufacturing Process, Manufacturing Tolerances and Applications.*
Expanded Metal Manufacturers Association http://www.naamm.org/emma/

SSMA : Steel Stud Manufacturers Association http://www.ssma.com/technical_library.aspx

PART I (For use by the Department or Agency)

How to Use This Guide

This Guide is intended to assist qualified security practitioners and departmental physical security staff to develop a Statement of Requirements (SOR) for the construction of a Secure Demising Wall (SDW).

Qualified architects or designers should be engaged to turn the SOR into detailed drawings and specifications – incorporating all client-specified features and components and ensuring that the design conforms to overall project requirements and all applicable codes and facility "fit-up" standards.

The rationale for any component or feature (as well as the purpose of a space or nature of the asset) should only be divulged to architects, designers or contractors on a need-to-know basis. They may require a security clearance to receive this information.

Segregation of details and distribution on a need-to-know basis will often be sufficient.
The architect or designer should be provided with formal guidance / direction on the preparation of drawings for tender or sub-trades to ensure that sensitive information is not inappropriately divulged. For example, the purpose or name of the room should not appear on widely disseminated drawings, specifications or other contract documents. A generic or numeric name should be used. Sub-trades should receive only enough information to perform their work (eg: partial building drawings and system schematics which do not identify adjacent activities or security-related system details). Security requirements should be incorporated into contract documents where feasible to ensure enforceability.

General

For many years, various departments have been using portions of the construction specifications from the G1-029 Secure Room Guide[1] to construct walls around departmental space (e.g., in office towers), working spaces, operations rooms, High Security Zones, etc.

This guide was developed specifically for the construction of a secure demising wall and to help avoid inappropriate use of the Secure Storage Room Guide (see note 1). Having a name, abbreviation, definition and guide number specifically for a Secure Demising Wall (SDW) also makes it easier to reference source material without confusion.

The wall design in this Guide is a tested and recommended light weight construction to adequately mitigate the design-basis threat against typical government offices in standard urban settings. It provides moderate resistance to force attacks (including those using portable cutting tools) and very good detection of such attacks (when approved vibration detection equipment is installed as recommended). This wall construction is not appropriate where a TRA has identified

[1] The Secure Room Guide G1-029 was updated in 2013 and renamed the G13-01 Secure Storage Room Guide to better reflect its intended application.

a need to provide an assured resistance to entry by sustained force attacks. UL-rated vaults or custom-designed barriers should be considered for such situations.

Application

Secure Demising Walls (SDW) are suitable for physically separating an Operations Zone from a Public/Reception Zone, or (when recommended in a TRA) to separate a Security Zone from an Operations zone or compartmentalize within a particular zone.

Secure Demising Walls facilitate detection and provide a delay to permit interception by an *appropriate* response within a reasonable time. It should be stressed that a rapid and appropriate response is key to the effectiveness of any delay and detection/ alarm security system.

Sound Reduction

An SDW was not designed for speech security and should never be the separation between a Sensitive Discussion Area (SDA) and a Public Zone. An SDA should be a room located in a Security Zone (whose perimeter walls may be a SDW).

However, sound reduction should normally be included to reduce nuisance noise and minimize the opportunistic overhearing of conversations which - although not classified - may still be considered sensitive.
Construction resulting in an STC of 54-55 dB is generally adequate for SDW applications.

The following assembly will provide an STC rating of approximately 54-55:

• Two layers of 16 mm fire-rated gypsum board
• One layer of sheet or expanded mesh steel
• Steel studs spaced 300 mm oc
• 150 mm thick glass fiber batts between studs
• Resilient metal channels spaced 400 mm apart
• One layer of 16 mm fire-rated gypsum board

This rating is for the wall assembly without pass-throughs or gaps. Acoustic caulking must be applied between the gypsum board and all adjacent surfaces to prevent sound leakage through spaces and gaps.

Doors installed with typical commercial seals (or acoustic seals improperly installed or adjusted) will generally not provide better than 35 dB sound reduction even when the doors are acoustically rated. As the intent of a SDW is not acoustic isolation (and many applications will involve commercial architectural doors and windows for visibility, public impact and accessibility), this should not be an issue. Vestibules can be helpful.

Fire Protection

Double panel or Type X drywall sheets may be installed as required to meet fire code requirements. Friction fit (batt) insulation must be used. Sprayed-on insulation must not be used as it may interfere with the transmission of vibrations along the sheet steel.

Slab-to-Slab

Secure Demising Walls should be slab-to-slab, i.e., from the finished structural floor to the underside of the structural roof /ceiling. Where roofs or floors are of wood or steel frame construction they should be steel reinforced the same as the walls. Where this is not feasible, other mitigation measures will be required. For guidance regarding the construction of a secure ceiling or floor, please contact the RCMP.

Secure Demising Wall Built Adjacent to Another Wall

When building Secure Demising Walls adjacent to non-departmental walls (e.g. leased spaces where modifications to the existing walls are not permitted under the occupancy instrument), the protective material will need to be installed on the secure (inside) side of the wall and all electrical and alarm wiring should be in surface-mounted conduit.

Ducts and Other Service Penetrations

Minimize ducts and service pass-throughs in Secure Demising Walls where possible. Do not locate pass-throughs in the Critical Attack Area around doors. Where pass-throughs are required, openings should be framed with studs to within 1” (25mm) of the pipe/conduit and the pipe or conduit secured to the stud framing at minimum two places. The wall protection material should be extended to within ¾” (20 mm) of the edge of the opening. Extend gypsum wall board to the edge of the pipe or conduit. Caulk all gaps with fire rated sealant. Recommended standard: ASTM E 814 (UL 1479) and CAN/ULC S115 or as required by the AHJ.

Where necessary to accommodate pipe or conduit movement or expansion, pipes and conduits may be enclosed in a close-fitting sheet metal sleeve and the sleeve mechanically fastened to the stud framing at minimum two places. Clearance between the sleeve and the pipe or conduit should be kept to a minimum and not exceed ¼”.

Steel bars (see Figures 8 & 9) should be installed in ducts in Public or Reception Zones to delay access of a person through a duct. They may be omitted if it is determined in a TRA that it is not a viable threat due to other security controls. Note that Man Bars do not prevent possible destruction, modification or interruption to assets within by introduction of water or other material through a duct. If a TRA identifies such threats, all ducts and openings may require additional mitigation measures (e.g.: filters or dampers).

Vibration Detector

While the sheet steel on the walls provides moderate force resistance, one of the main reasons for the steel sheets on the wall is to transmit vibrations from force attacks to vibration sensors. A

volumetric intrusion detection sensor (e.g. motion sensor) located in the room or space is also recommended, but will not detect the adversary until he/she has already defeated the SDW, doors, windows or components and gained entry. As the purpose of intrusion detection is to generate a response in time to intercept the adversary, detection only upon entry reduces the available response time.

The RCMP has tested and approved a vibration detector for use with the SDW, which is listed in the G1-001 Security Equipment Guide (SEG). To ensure detection as per approval testing, the detectors must be installed directly on the steel at a stud/ joist using the base plates provided by the manufacturer.

Sensors should be spaced following the manufacturer's recommended spacing with at least one sensor per wall segment to ensure good attack detection. A sensor should also be installed on the door (in addition to a magnetic contact switch to detect if a door is opened surreptitiously) to ensure good detection of cutting or pounding attacks against the door/lock.

Doors, Locks and Windows

Doors and windows installed in a SDW should provide moderate resistance to force attacks. Options may include: burglar-resistant glazing, security films, exterior security grilles or screens (typically of expanded metal mesh on steel frames) or lockable steel rolling window shutters. Due to the wide diversity of products and applications, the RCMP has not developed standard guidance for these items.

Statement of Requirements

Where the department (client) is not also the Designer, a Statement of Requirements (SOR) should be developed to tell the Designer exactly what is required and to identify selected construction options from those presented in the General Specifications in Part II.

The SOR and all documentation leading to the selection of room or wall specifics should be considered sensitive and treated accordingly.

Do not tell the designer why a selection has been made unless the designer has a need to know.

PART II – SDW Construction Specifications

Note: The specifications in this Part should be modified as required and incorporated into the Project Contract Documents by the Designer in accordance with client requirements (ideally outlined in a detailed SDW Statement of Requirements) and overall project and code requirements.

Wall Framing (figure 1)

Extend wall partition framing slab to slab.

Top and Bottom Tracks:
SSMA standard: 1- 5/8” x 6”, 18 ga (600T162-43);
or 2” x 6”, 18 ga (600T200-43) (Preferred option)
Secure top and bottom steel tracks to both slabs at 300mm oc using any expanding (preferably double expanding) mechanical fastener. Non-expanding screws (e.g., Tapcon) are not acceptable.

Studs:
SSMA standard: 1- 5/8” x 6”, 18 ga (600S162-43: 33ksi); or
2” x 6”, 18ga (600S200-43: 33ksi) (preferred option)
Space studs at 300 mm oc and secure to the top and bottom track with welds or rivets (not screws).

Install double (jamb) studs at the door frame opening. Install the door frame as per HMMA 840-07 part 3 A, B, C, D and E (except that screws shall be replaced with steel rivets).

Install anti-spread bracing approximately 48” from the bottom of the wall between door frame double stud and the adjacent stud on both sides of the frame.

Construct wall corners with double studs.

Note: Leaving a small gap and using drywall sheets to brace frame sections during wall erections is permitted provided steel sheets on attack side are continuous over all gaps.

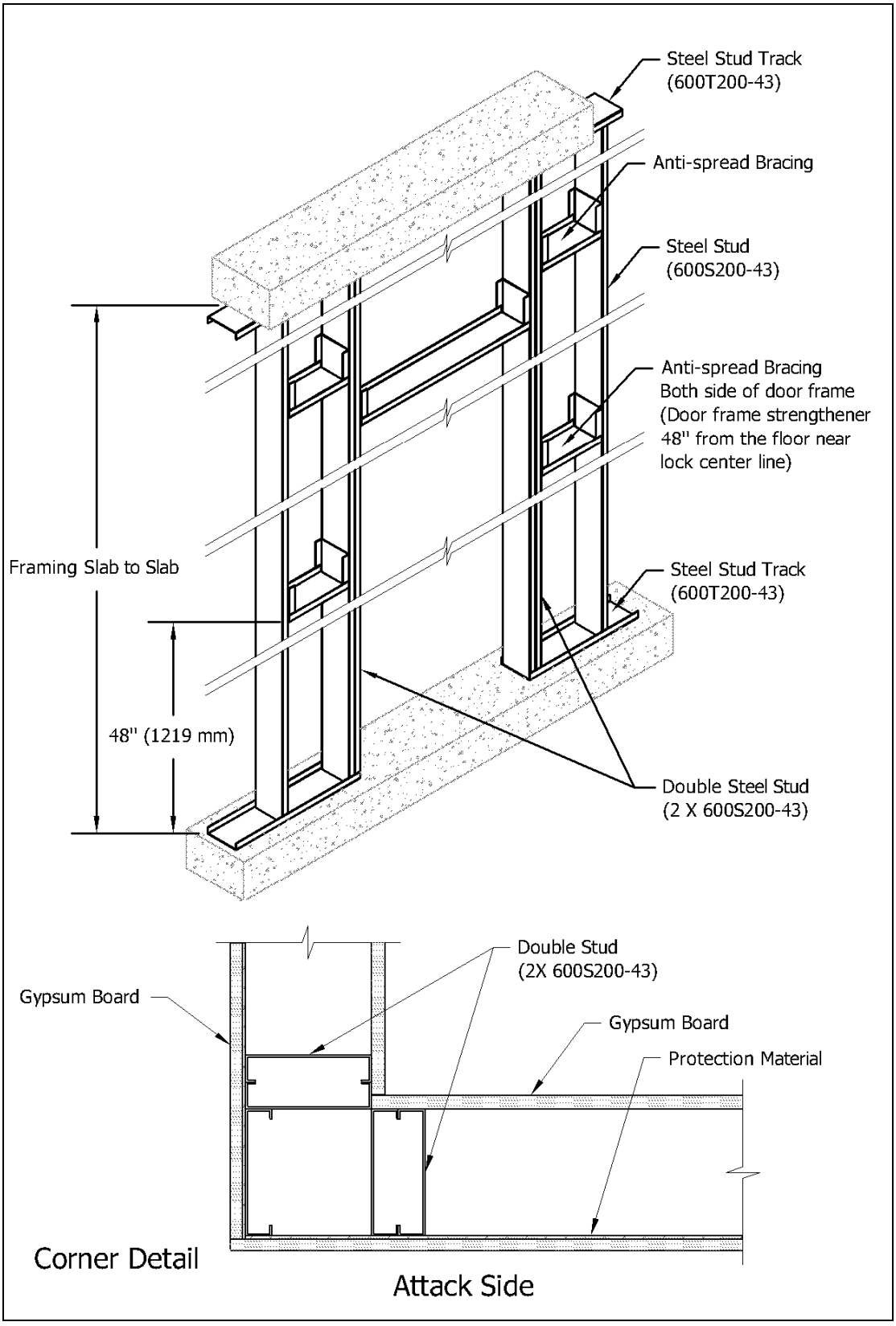


Figure 1: Wall Construction

Wall Protection Material (Figures 2 to 4)

Wall protection material may be one of two options:

Flattened Metal Mesh: To EMMA 557-99. Style ¾-9F: nominal strand thickness of 0.120" (0.108" in to 0.132"). Diamond opening of 0.563" x 1.688".
OR
Sheet Steel: 16 ga A1008 / A1008M (cold rolled) or A1011/ A1011M (hot rolled) or equivalent.

Mount on outside (attack side) of the room. Support all edges by anti-spread bracing, studs or corners. Align the sheet edges at every vertical and horizontal seam on the centre line of the steel stud or anti-spread bracing and secure all sheets with welds or rivets.

Note: Screws (including "security screws") are **NOT** acceptable for permanently attaching the protection material (steel or steel mesh). Screws may be used to "tack" the sheets in place pending riveting or welding. Temporary screws do not need to be removed.

Welding (Alternate Method)

Steel mesh (Figure 2): 3mm fillet weld along the strand at 200mm oc

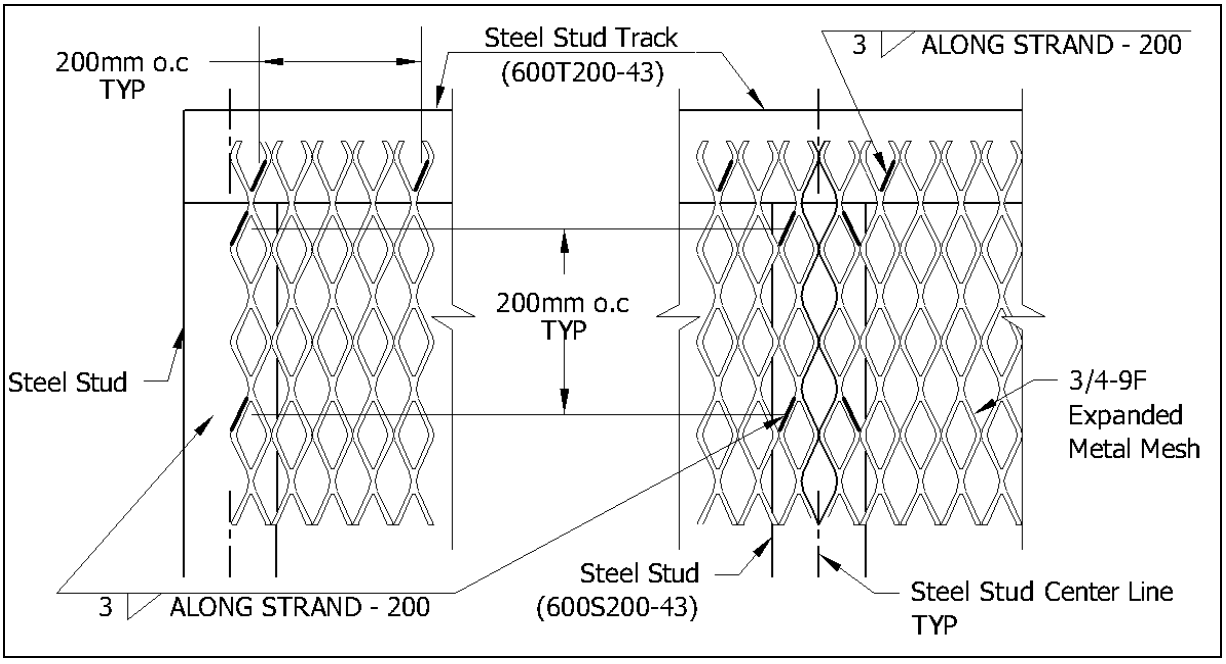


Figure 2: Welding Steel Mesh

Steel Sheet (Figure 3): 1.5mm fillet weld 15mm long at 200mm oc **or**
8mm plug weld at 200mm oc

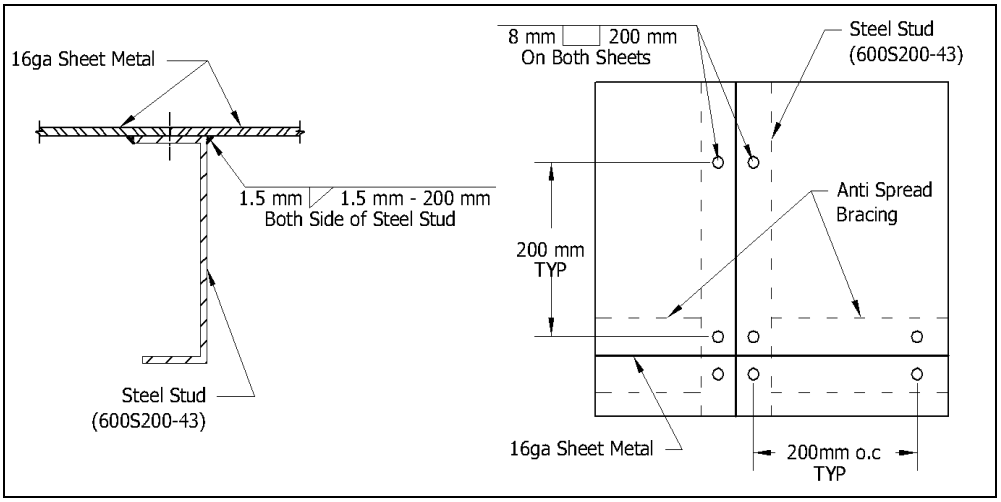


Figure 3: Welding Sheet Steel

Rivets (Preferred Method)

Steel sheet: 3/16" Steel rivets at 200mm oc
Steel mesh: 3/16" Steel rivets and "fender" washer (1 ½" OD, 3/16" ID) at 200mm oc

Suggested material:
Rivets: 3/16" Steel pop rivet: Speaneur part #301-440
Washers: 1 ½" OD, 3/16" ID "fender" washer: Fastenal part #1133204

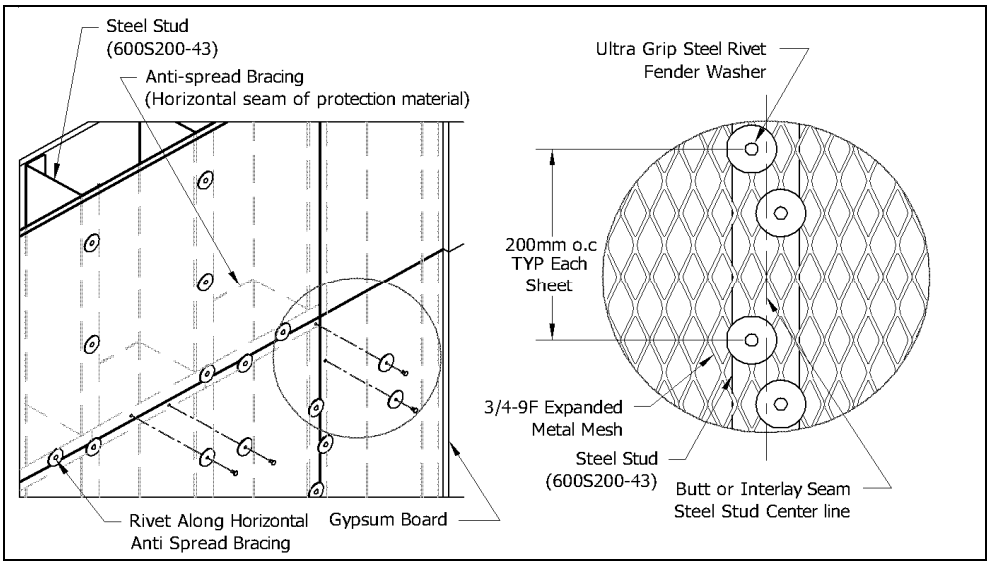


Figure 4: Riveting sheet or mesh

Figure 5: Example of mesh interlay seam, riveted

Critical Attack Area (Figure 6)

Install 16 ga sheet steel on the inside of the room and extend 1200 mm from the edge of the door frame. Attach as per rivet or welding requirements for selected method.

Note: Perforations for services, conduit or ducts are not permitted in the critical attack area.

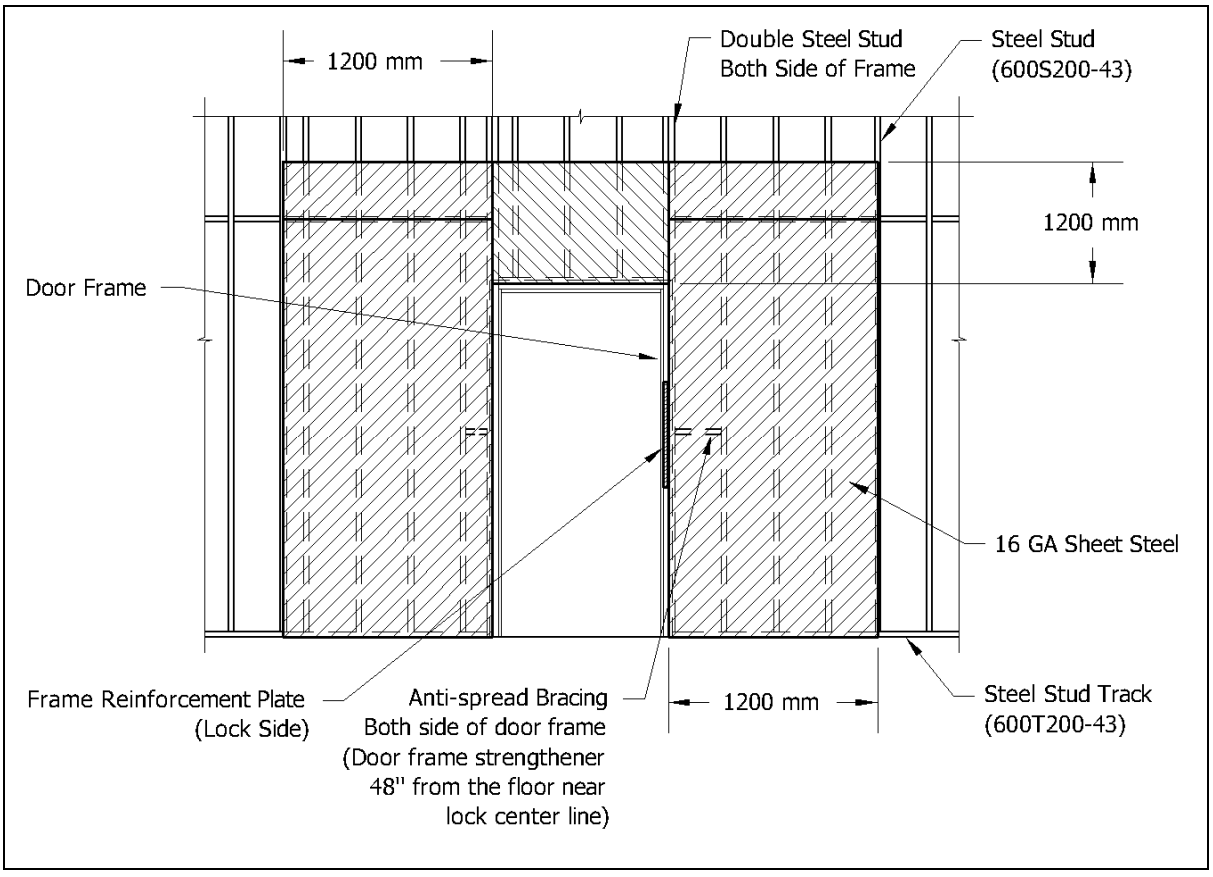


Figure 6: Critical Attack Area Wall Reinforcement

Wall Finishing Details

Attach drywall on both sides using standard drywall screws.
Apply fire-rated sealant continuously on both sides of the top and bottom of partition.
ASTM E814 (UL1479), ASTM E1966 (UL 2079) or CAN/ ULC S115 test standards with a fire/ smoke rating acceptable to the Authority Having Jurisdiction (AHJ).

Paint exterior surface of wall slab-to-slab. Paint must be uniform and without blemishes. Joints must not be visible.
Recommended: 1 coat primer/sealer and 1 coat alkyd, gloss enamel conforming to CAN/CGSB-1.60.

Frame Reinforcement at Door (where appropriate): (Figure 7)

Secure a 6.4 mm x 25 mm x 610 mm steel plate inside the frame and align centre with the lock bolt.

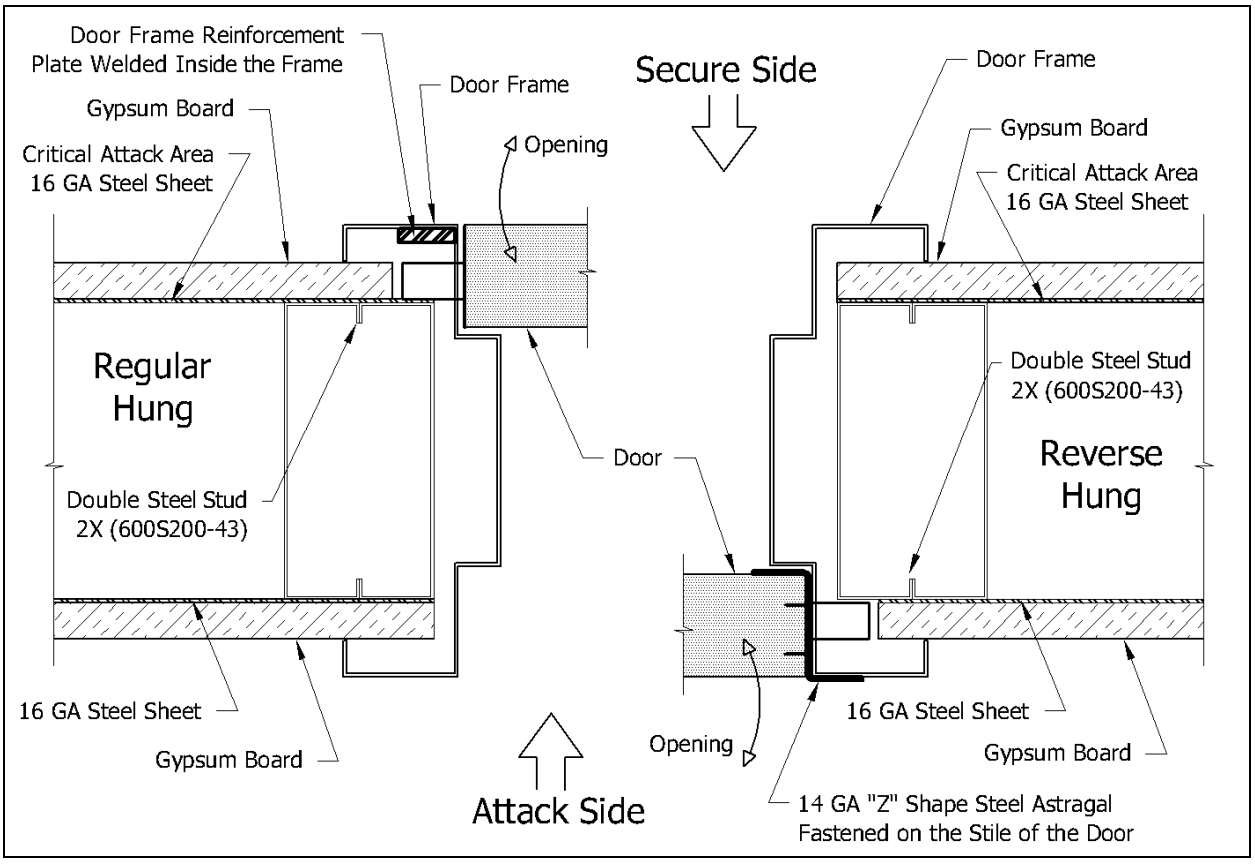


Figure 7: Frame Reinforcement at Door

Ventilation Duct Pass-throughs

Note: Where superior resistance to cutting is required, steel bars can be specified as tool-resistant steel (grade 1 or 2) per ASTM A627.

Ceiling mount: (Figure 8)

1. The duct sleeve must be at least same thickness as the duct passing through.
2. The overall dimension of the sleeve must be slightly greater than the duct.
3. Construct frames of 1- 3/8” x 1- 3/8” x 1/8” angle steel welded around duct sleeve (ceiling mount brackets are recommended).
4. Space 3/8” Ø steel bars at 6” oc and weld to the frame.
5. Secure the duct sleeve to the structural ceiling with mechanical fasteners.
6. Cut protection material ¾” max from the edge of the duct opening (3 sides).
7. Apply fire-rated caulking between duct sleeve and finished wall.

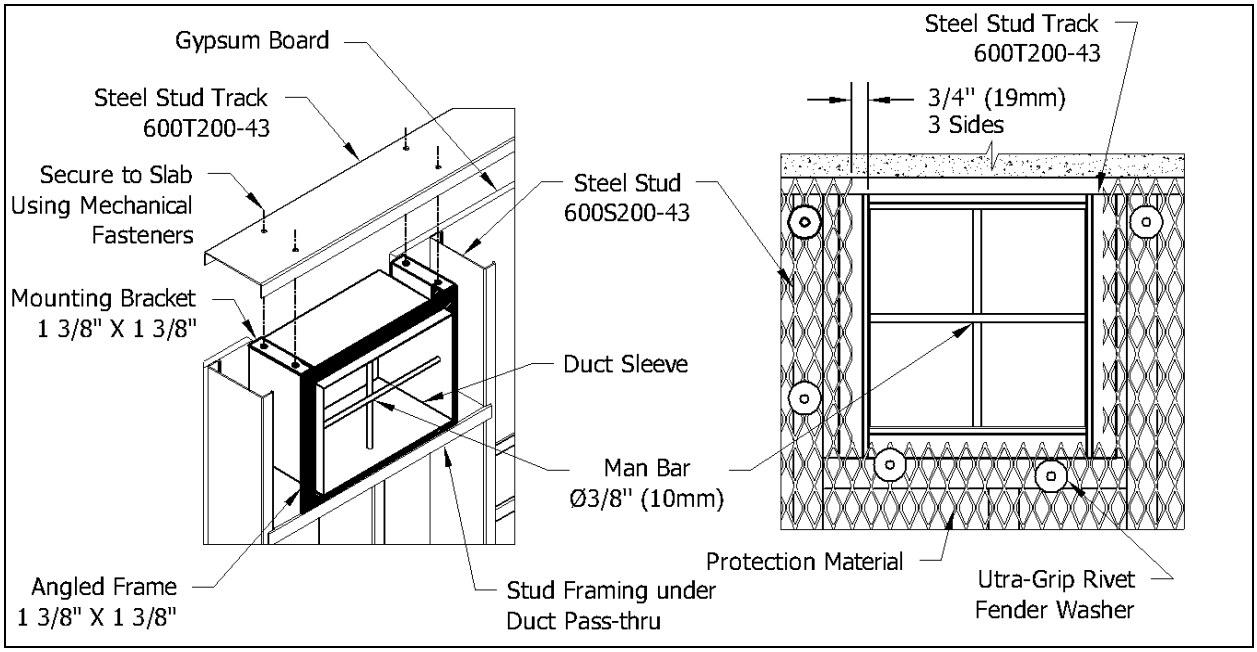


Figure 8: Ceiling Mount Duct Pass-through

Surface mount: (Figure 9)

1. The duct sleeve must be at least the same thickness as the duct passing through.
2. The overall dimension of the sleeve must be slightly greater than the duct.
3. Construct frame on each side of the wall of 1- 3/8” x 1- 3/8” x 1/8” angle steel welded around duct sleeve.
4. Space 3/8” diameter steel bars at 6’’ oc and weld to the frame.
5. Secure duct sleeve with ¼” diameter bolts and hex nuts (inside the room) at 8” oc around the outside duct sleeve. The bolt head shall be on the attack side and be welded in at least three places to the angle frame.
6. Framing around duct sleeve is required.
7. Apply fire-rated caulking between duct sleeve and finished wall.

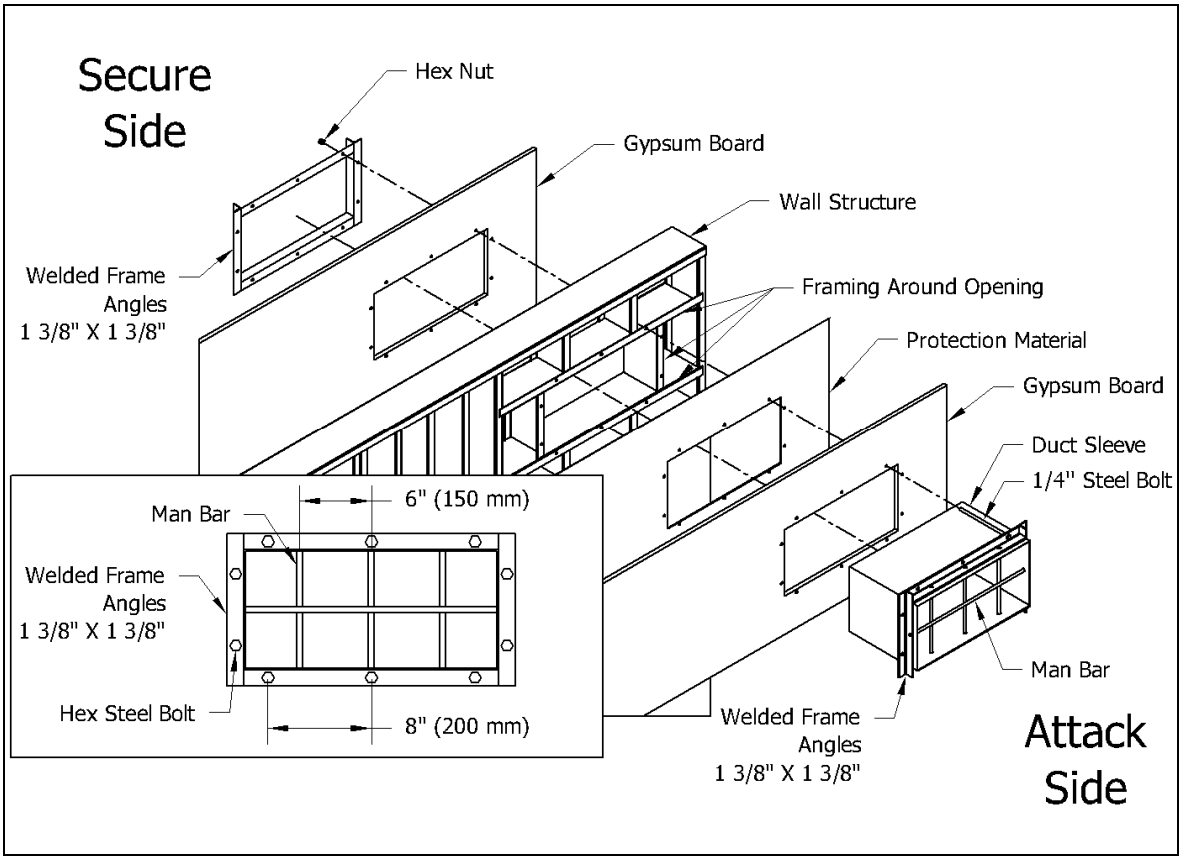


Figure 9: Surface Mount Duct Pass-through

Advice and Guidance

Royal Canadian Mounted Police
Departmental Security Branch
Physical Security Section
1426 St. Joseph Boulevard
Ottawa, Ontario K1A 0R2
Email: Sec-Equip@rcmp-grc.gc.ca