



Comparison of the Canadian *Industrial Security Manual* and the United States *National Industrial Security Program Operating Manual*

Andrew Hammond

Constella Health Sciences, Atlanta, Georgia

Abstract

Because of the potential for use as a bioterrorism agent or bioweapon, many governments have imposed strict regulations regarding the possession, use, and transfer of “select” biological agents. Consequently, much of the information surrounding the possession and use of these agents is potentially classified, and those contractors and their employees who require access to this information must receive Facility (contractor) and Personnel (employees) clearances. Both Canada and the United States (U.S.) have produced industrial security manuals—the Industrial Security Manual (ISM) (Canadian and International Industrial Security Directorate, 2004) and the National Industrial Security Program Operating Manual (NISPOM) (Defense Technical Information Center, 1995)—for use by cleared government contractors. These documents set forth the requirements, restrictions, and other safeguards that are necessary to prevent unauthorized disclosure of classified information and assets provided to or produced by private government contractors. This article compares and contrasts the requirements set forth in the ISM and the NISPOM. The results of this comparison present a valuable security management tool for private organizations that wish to engage in classified work for the Canadian, U.S., or both governments.

Introduction

As a result of the October 2001 anthrax letter attacks, both the United States and Canada enacted new laws imposing additional restrictions on certain hazardous biological agents and toxins. The U.S. enacted the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (Public Law 107-188) (U.S. Government Printing Office, 2002) and Canada passed the Public Safety Act, 2002 (Parliament of Canada, 2002). Because of the potential for “select” biological agents and toxins being used as bioterrorism agents or in a bioweapons program, both Acts impose strict regulations regarding their possession, use, and transfer. Consequently, much of the information surrounding the possession and use of these agents is potentially classified (or confidential), and those organizations and their employees who require access to this information must receive Facility (organization) and Personnel (employee) clearances. Both Canada and the U.S. have produced industrial security manuals—*Industrial Security Manual (ISM)* (Canadian and International Industrial Security Directorate, 2004) and the *National Industrial Security Program Operating Manual (NISPOM)* (Defense Technical Information Center, 1995)—for use by cleared government contractors. These documents set forth the requirements, restrictions, and other safeguards that are necessary to prevent unauthorized disclosure of classified information (and assets) provided to or produced by private

government contractors and to control the authorized disclosure of classified information (and assets) released by the governments to their contractors.

United States—National Industrial Security Program Operating Manual

Security Classifications

An original classification decision at any level can be made only by a U.S. Government official who has been delegated this authority in writing. Contractors may make derivative classification decisions based on the guidance provided by the Contract Security Classification Specification that is issued with each classified contract. Derivative classification is the act of classifying a specific item of information or material on the basis of an original classification decision already made by an authorized original classification authority. The source of authority for derivative classification ordinarily consists of a previously classified document or a classification guide issued by an original classification authority.

Top Secret

Top secret information or material is that information or material whose unauthorized disclosure could be reasonably expected to cause *exceptionally grave damage* to the national security that the original classification authority is able to identify or describe. Examples include armed hostilities against the United States or its allies, disruption of foreign relations vitally affecting the national security, and the disclosure of scientific or technological developments vital to national security.

Secret

Secret information or material is that information or material whose unauthorized disclosure could be reasonably expected to cause *serious damage* to the national security that the original classification authority is able to identify or describe. Examples of serious damage include significant impairment of a program or policy directly related to the national security and compromise of significant scientific or technological developments relating to national security.

Confidential

Confidential information or material is that information or material whose unauthorized disclosure could be reasonably expected to cause *damage* to the national security that the original classification authority is able to identify or describe. Examples include documents relating to clearance or assignment of personnel who will have knowledge of, or access to, classified information or materials or details pertaining to features of routes and schedules of shipments of confidential materials.

Facility Security

Facility Clearances

A facility security clearance (FCL) is an administrative determination that a facility is eligible for access to classified information at the same or lower classification category as the clearance being granted. Contractors are eligible for custody of classified material, if they have an FCL and storage capability approved by the Cognizant Security Agency (CSA).

A procuring activity of the Government or cleared contractor may request a facility clearance for a contractor or prospective contractor/subcontractor when a definite, classified procurement need has been established. Also, the contractor must be organized and existing under the laws of any of the 50 states, the District of Columbia, or Puerto Rico, and be located in the U.S. and its territorial areas or possessions.

Meetings

Classified disclosure at a meeting (e.g., conference, seminar, symposium, exhibit, convention, training course, or other such gathering) which serves a government purpose and at which adequate security measures have been provided in advance may be conducted by a cleared contractor provided the meeting is authorized by a Government Agency that has agreed to assume security jurisdiction. The Government Agency must approve security arrangements, announcements, attendees, and the location of the meeting. (Classified meetings shall be held only at a Federal Government installation or a cleared contractor facility where adequate physical security and procedural controls have been ap-

proved.) Contractors wishing to conduct classified meetings shall submit their requests to the Government Agency having principal interest in the subject matter of each meeting.

Personnel Security

Security Officers

The Facility Security Officer (FSO) shall be a U.S. citizen employee appointed by the contractor who is cleared as part of the facility clearance. The FSO will supervise and direct security measures necessary for implementing the *NISPOM* and related Federal requirements for classified information.

The senior management official and the FSO must always be cleared to the level of the Facility Clearance (FCL). Other officials, as determined by the CSA, must be granted a Personnel Clearance (PCL) or be excluded from classified access.

Personnel Clearances

An industrial personnel security clearance is an administrative determination that an industrial employee is eligible for access to classified information. This determination is based on investigation and review of available personal data and a finding that access is clearly consistent with national interests.

An individual may be processed for a personnel security clearance only when employed by a cleared contractor in a job requiring access to classified information. As an exception, a candidate for employment may be processed for a PCL provided a written commitment for employment that prescribes a fixed date for employment within the ensuing 180 days has been made by the contractor, and the candidate has accepted the employment offer in writing.

Under rare circumstances, a non-U.S. citizen may be issued a Limited Access Authorization for access to classified information. Specific criteria and limitations are provided in the *NISPOM*.

Contractors have no authority to grant, deny, or revoke personnel clearances for their employees. This authority is reserved by the U.S. Government.

Subcontracting

Before a prime contractor may release, disclose classified information to a subcontractor, or cause

classified information to be generated by a subcontractor, he or she must determine the security requirements of the subcontract and determine clearance status of prospective subcontractors. The prime contractor shall verify the clearance status and safeguarding capability of the subcontractor from the CSA. If a prospective subcontractor does not have the appropriate FCL or safeguarding capability, the prime contractor shall request the CSA of the subcontractor to initiate the necessary action.

The prime contractor shall ensure that a Contract Security Classification Specification is incorporated in each classified subcontract. The contractor shall also review the security requirements during the different stages of the subcontract and provide the subcontractor with applicable changes in these security requirements. Upon completion of the subcontract, the subcontractor may retain classified material received or generated under the subcontract for a 2-year period, provided the prime contractor or GCA does not advise to the contrary.

Education, Training, and Briefings

Contractors shall provide all cleared employees with security training and briefings commensurate with their involvement with classified information. Contractors shall also be responsible for ensuring that the FSO, and others performing security duties, complete security training deemed appropriate by the CSA. (Training, if required, should be completed within 1 year of appointment to the position of FSO.) The contractor is responsible for providing all cleared employees with some form of security education and training at least annually.

The SF 312 is an agreement between the United States and an individual who is cleared for access to classified information. An employee issued an initial PCL must execute an SF 312 prior to being granted access to classified information. The employee must also receive an initial security briefing that includes a Threat Awareness Briefing, a Defensive Security Briefing, an overview of the security classification system, employee reporting obligations and requirements, and security procedures and duties applicable to the employee's job.

Contractors shall debrief cleared employees at the time of termination (discharge, resignation, or

retirement); when an employee's PCL is terminated, suspended, or revoked, and upon termination of the FCL.

Visits

The contractor must determine that the visit is necessary and that the purpose of the visit cannot be achieved without access to, or disclosure of, classified information. All classified visits require advance notification to, and approval of, the organization being visited. In urgent cases, visit information may be furnished by telephone provided that it is followed up in writing. The contractor shall issue a Visit Authorization Letter (VAL) to the organization being visited that shall include the following:

- Contractor's name, address, and telephone number, assigned CAGE Code, and certification of the level of the FCL
- Name, date, place of birth, and citizenship of the employee intending to visit
- Certification of the proposed visitor's PCL and any special access authorizations required for the visit
- Name of person(s) to be visited
- Purpose and sufficient justification for the visit to allow for a determination of the necessity of the visit
- Date or period during which the VAL is to be valid

Contractors shall maintain a record of all visitors to their facility who have been approved for access to classified information.

Document Security

General Marketing

All classified material shall be marked on the face of the document to show the name and address of the facility responsible for its preparation and the date of preparation. The highest level of classified information contained in a document is its overall marking. The overall marking shall be conspicuously marked or stamped at the top and bottom on the outside of the front cover, on the title page, on the first page, and on the outside of the back cover. Interior pages of classified documents shall be marked at

the top and bottom with the highest classification of the information appearing thereon or marked UNCLASSIFIED if all the information on the page is UNCLASSIFIED. The major components of complex documents are likely to be used separately. Therefore, each major component shall be marked as a separate document. Also, each section, part, paragraph, or similar portion of a classified document shall be marked to show the highest level of its classification, or that the portion is unclassified. Unclassified subjects and titles shall be selected for classified documents, if possible. If a classified subject or title must be used, it shall be marked with the appropriate symbol—(TS), (S), or (C)—placed immediately following and to the right of the item.

All classified information shall be marked to reflect the source of the classification and declassification instructions. This required information shall be placed on the cover, first page, title page, or in another prominent position.

General Storage

Cognizant security officials shall work to meet appropriate security needs according to the intent of the NISPOM and at an acceptable cost.

TOP SECRET material shall be stored in a GSA-approved security container, an approved vault, or an approved Closed Area. Supplemental protection is required.

SECRET material shall be stored in the same manner as TOP SECRET material without supplemental protection.

CONFIDENTIAL material shall be stored in the same manner as TOP SECRET or SECRET material except that no supplemental protection is required.

Reproduction

Contractors shall establish a reproduction control system to ensure that reproduction of classified material is held to the minimum consistent with contractual and operational requirements. Classified reproduction shall be accomplished by authorized employees knowledgeable about the procedures for classified reproduction. The use of technology that prevents, discourages, or detects the unauthorized reproduction of classified documents is encouraged.

All reproductions of classified material shall be conspicuously marked with the same classification markings as the material being reproduced.

Domestic Transmission Standards (Outside of Facility)

Top Secret

- Written authorization of the Government Contracting Activity (GCA)
- Sealed, opaque inner and outer covers with the inner cover being a wrapper or envelope plainly marked with the assigned classification and addresses of both sender and addressee
- A receipt that identifies the sender, the addressee, and the document shall be attached to or enclosed in the inner cover
- Via:
 - a. Defense Courier Service (DCS), if authorized by GCA
 - b. A designated courier or escort cleared for access to TOP SECRET information
 - c. By electrical means over CSA-approved secured communications security circuits provided such transmission conforms with the NISPOM, the telecommunications security provisions of the contract, or is authorized by the GCA

Secret

- Sealed, opaque inner and outer covers with the inner cover being a wrapper or envelope plainly marked with the assigned classification and addresses of both sender and addressee
- A receipt that identifies the sender, the addressee, and the document shall be attached to or enclosed in the inner cover
- Via:
 - a. TOP SECRET methods
 - b. USPS Express or Registered mail
 - c. A cleared "Commercial Carrier"
 - d. A cleared commercial messenger service engaged in the intracity/local area delivery (same day delivery only) of classified material
 - e. A commercial delivery company approved by the CSA
 - f. Other methods as directed, in writing, by the GCA

Confidential

- Packaged by SECRET material methods except that a receipt is required only if the sender deems it necessary
- Via:
 - a. SECRET methods
 - b. USPS Certified mail

International Transmission Standards

Top Secret

- Domestic requirements
- Via:
 - a. Defense Courier Service
 - b. Department of State Courier System
 - c. Courier service authorized by GCA

Secret and Confidential

- Domestic requirements
- Via:
 - a. Registered mail through U.S. Army, Navy, or Air Force postal facilities
 - b. Appropriately cleared contractor employee
 - c. U.S. civil service employee or military person designated by the GCA
 - d. U.S. and Canadian registered mail with registered mail receipt to and from Canada and via a U.S. or Canadian government activity
 - e. As authorized by the GCA

Destruction

Contractors shall destroy classified material in their possession as soon as possible after it has served the purpose for which it was intended.

Classified material may be destroyed by burning, shredding, pulping, melting, mutilation, chemical decomposition, or pulverizing. Pulpers, pulverizers, or shredders may be used only for the destruction of paper products. Residue shall be inspected during each destruction to ensure that classified information cannot be reconstructed. Crosscut shredders shall be designed to produce residue particle size not exceeding 1/32 inch in width by 1/2 inch in length.

Public destruction facilities may be used only with the approval of the CSA, and classified material removed from a cleared facility for destruction shall be destroyed on the same day it is removed.

Destruction shall be performed only by appropri-

ately cleared employees of the contractor. For destruction of TOP SECRET material, two persons are required. For destruction of SECRET and CONFIDENTIAL material, one person is required.

Destruction records that indicate the date of destruction, identify the material destroyed, and are signed by the individuals designated to destroy and witness the destruction are required for TOP SECRET material.

Information System Security

Information systems (IS) that are used to capture, create, store, process, or distribute classified information must be properly managed to protect against unauthorized disclosure of classified information and loss of data integrity, and to ensure the availability of the data and system.

Protection requires a balanced approach including IS security features to include, but not limited to, administrative, operational, physical, computer, communications, and personnel controls. Protective measures commensurate with the classification of the information, the threat, and the operational requirements associated with the environment of the IS are required.

The requirements outlined in the *NISPOM* apply to all information systems processing classified information. Additional requirements for high-risk systems and data are covered in the *NISPOM Supplement*.

The CSA is the Designated Accrediting/Approving Authority (DAA) responsible for accrediting information systems used to process classified information in industry. A formal certification and accreditation (C&A) occurs after the protection measures have been implemented and any required IS protection documentation has been approved. Certification validates that the protection measures described in the System Security Plan (SSP) have been implemented on the system and that the protection measures are functioning properly. Accreditation is the approval by the CSA for the system to process classified information.

Canada—Industrial Security Manual

Security Classifications

The originator of the information and assets determines the classification level.

Top Secret

TOP SECRET refers to information and assets related to the national interest that may qualify for an exemption or exclusion under the Access to Information Act or Privacy Act and that the compromise of which would reasonably be expected to cause *exceptionally grave injury* to the national interest.

Secret

SECRET refers to information and assets related to the national interest that may qualify for an exemption or exclusion under the Access to Information Act or Privacy Act and that the compromise of which would reasonably be expected to cause *serious injury* to the national interest.

Confidential

CONFIDENTIAL refers to information and assets related to the national interest that may qualify for an exemption or exclusion under the Access to Information Act or Privacy Act and that the compromise of which would reasonably be expected to cause *injury* to the national interest.

Protected “C”

PROTECTED “C” refers to information and assets related to other than the national interest that may qualify for an exemption or exclusion under the Access to Information Act or Privacy Act that could reasonably be presumed to cause *extremely serious injury*, such as loss of life, if compromised.

Protected “B”

PROTECTED “B” refers to information and assets related to other than the national interest that may qualify for an exemption or exclusion under the Access to Information Act or Privacy Act that could reasonably be expected to cause *serious injury* if compromised.

Protected “A”

PROTECTED “A” refers to information and assets related to other than the national interest that may qualify for an exemption or exclusion under the Access to Information Act or Privacy Act that could reasonably be presumed to cause *injury* if compromised.

Facility Security

Facility Clearances

A *Facility Security Clearance* is an administrative determination that an organization is eligible, from a security viewpoint, for access to CLASSIFIED and PROTECTED information and assets of the same or lower classification level as the clearance being granted.

There are three types of Facility Security Clearances each of which may be authorized at the classification level of CONFIDENTIAL, SECRET, or TOP SECRET:

1. *Personnel Assigned* (PA). This is the most basic type of Facility Security Clearance which involves security screening of the organization’s Key Senior Officials and employees. There is NO requirement to evaluate the physical security status of the organization’s facilities. The organization is not authorized to possess or store CLASSIFIED information and assets.
2. *Document Safeguarding Capability* (D.Sc.). In addition to the security screening of the organization’s Key Senior Officials and employees, the physical security of the organization’s facilities is assessed to ensure safeguarding requirements are met. The organization is authorized to possess and store CLASSIFIED information and assets.
3. *Production* (PROD). This includes all of the elements of a Document Safeguarding Facility Security Clearance. In addition, the security of the manufacturing, repairing, modifying, or otherwise working on CLASSIFIED components or items is assessed to ensure government security requirements are met.

A *Designated Organization Screening* (at the PROTECTED level) is an administrative determination that an organization is eligible, from a security viewpoint, for access to PROTECTED information and assets of the same or lower level as the clearance be-

ing granted. The three types of Designated Organization Screening are equivalent to the three types of Facility Security Clearances except they pertain only to PROTECTED information and assets. Each of the three types may be authorized at one of the following levels: PROTECTED “A,” PROTECTED “B,” or PROTECTED “C.”

An organization is eligible to obtain an organization security screening/clearance only if it is sponsored by an authorized sponsor in support of an existing or impending contract or bid solicitation which calls for access to CLASSIFIED/PROTECTED information, assets, and/or certain restricted work sites.

Meetings

(No provisions are established within the Canadian *Industrial Security Manual*.)

Personnel Security

Security Officers

All organizations that require a Designated Organization Screening or a Facility Security Clearance shall appoint a *Company Security Officer*. The Company Security Officer shall be appointed by the Chief Executive Officer (CEO) or the designated *Key Senior Official* (KSO) of the organization. The CSO must be a Canadian citizen employee, report to a designated KSO, and be security screened or cleared to the Reliability Status level or Facility Security Clearance level of the facility. The appointment of the Company Security Officer must be approved by the Canadian and International Industrial Security Directorate (CIISD).

When a facility-cleared Canadian parent organization owns one or more cleared subsidiaries in Canada, a *Corporate Company Security Officer* (CCSO) should be appointed to oversee government industrial security matters for the entire corporation.

Personnel Clearances

Personnel Security Screening must be carried out according to the highest sensitivity level of information and assets that will be accessed during the

contracting process and/or required for access to restricted work sites. Access to PROTECTED information, assets, and restricted work sites requires that an individual has *Reliability Status*, and access to CLASSIFIED information, assets, and/or restricted work sites requires a *Security Clearance* at the appropriate level of sensitivity.

Only individuals employed or under a contract to commence employment within 60 days by a private sector organization on a contract/subcontract requiring access to CLASSIFIED/PROTECTED information, assets, and/or certain restricted work sites may be security screened. Non-Canadian citizens may be security cleared with access limitations. The limitations include denying access to CLASSIFIED/PROTECTED information and assets which are not of Canadian origin, do not come from the country of which the person is a citizen, or are not releasable to his/her nation of origin.

Contractors have no authority to deny or revoke Personnel Security Clearances for employees. This authority is reserved by the Canadian Government. The contractor may suspend the access of an individual, while notifying CIISD of the circumstances.

Subcontracting

Contractors shall subcontract work only to companies holding a current Designated Organization Screening or a Facility Security Clearance of the type and at the level appropriate to the work to be performed under the subcontract. CIISD approval of the subcontractor must be obtained before award of the subcontract and the Designated Organization Screening or Facility Security Clearance for the proposed subcontractor(s) must be verified by CIISD before issue of bid solicitation documents. Contractors shall not assign a subcontract to organizations located outside of Canada without the prior written approval of CIISD and the Public Works and Government Services Canada (PWGSC) contracting authority.

The prime contractor shall ensure the security safeguarding of work placed with subcontractors.

Education, Training, and Briefings

A major objective of the Company Security Officer in conducting a Security Education Program

involves working closely with management, from the top down, to ensure proper company security. Managers and supervisors at all levels are responsible not only for their own personal security measures, but also for ensuring that proper security procedures are followed by all employees in the organization. An initial security briefing, reinforced by an ongoing Security Education and Awareness Program, is essential to the maintenance of an effective security program.

Upon receiving a Personnel Security Clearance an employee acknowledges his or her responsibilities by reading and signing the Security Screening Certificate and Briefing Form, TBS/SCT 330-47 Rev. 2002/06. A briefing from the Company Security Officer, which details the individual's specific responsibilities and duties relative to security in the facility, must be presented. (New employees, even though not yet security-screened and therefore prohibited from access to CLASSIFIED information and assets, should be given a security briefing appropriate to their duties.)

Visits

A Visit Clearance Request (VCR) (submitted to CIISD via a Request for Visit form) is required when a security-cleared individual must visit a government/commercial organization in Canada or abroad, for the purpose of having access to CLASSIFIED information and assets or where access to the installation is restricted in the interest of national security. Visitors must not proceed with CLASSIFIED visits without prior visit clearance authorization from CIISD. The host organization shall deny access to CLASSIFIED information and assets or access to certain restricted work sites until the visitors' Personnel Security Clearance level and their need-to-know have been verified and confirmed by the CIISD through official visit protocol.

Submission of a VCR initiates verification by CIISD that confirms:

- The organization requesting the visit has an Facility Security Clearance to the required level
- Each of the proposed visitors has a valid Personnel Security Clearance to the required level
- Foreign disclosure limitations are identified and strictly observed

Visit Clearance Request is approved when the

requesting organization is notified by CIISD. Visitors must not proceed on CLASSIFIED visits without prior visit clearance authorization.

Visit Clearance Request (VCR) requires strict lead-times imposed by the authorities of foreign nations. Every effort must be made to ensure that lead-times are observed, as failure to do so will likely result in rejection of the RFV.

Organizations shall maintain a record of all individuals who visit the facility for the purpose of having access to CLASSIFIED information. This record shall be separate from the record of unclassified visits.

Document Security

General Marketing

All documents shall be marked on the outside of both the front and back covers with the highest level of classification and loose documents shall be marked on every sheet. Security markings should include the applicable classification/protection and the date or event at which declassification or downgrading is to occur. All covering or transmittal letters or forms or circulation slips must be marked to show the highest level of classification or protection of the attachments.

For TOP SECRET information, mark the classification in the upper right corner of each document page and show the total number of pages on each page of the document.

For SECRET information, mark the classification in the upper right corner of each document page.

For CONFIDENTIAL information, mark the classification in the upper right corner of the face of the document.

For PROTECTED information, mark the word "PROTECTED" in the upper right corner of the face of the document and, where required, with the letter "A," "B," or "C" to indicate the level of protection.

General Storage

PROTECTED B and PROTECTED C information and assets and all CLASSIFIED information must be stored in an approved security container.

PROTECTED A information and assets shall be stored in a locked container.

CLASSIFIED or PROTECTED information and assets may be stored on open shelving in a secure room, only after inspection and approval by CIISD and only to the level approved by CIISD. Also, CLASSIFIED and PROTECTED information and assets shall not be stored in the same container as negotiable or attractive assets.

Reproduction

Reproduction of CLASSIFIED information shall be done only with the authorization of the Company Security Officer or an authorized Alternate Company Security Officer. Reproductions must be marked, registered, and accounted for in the same manner as for the originals. Reproductions of PROTECTED information must be marked in the same manner as the originals. TOP SECRET and PROTECTED C information shall NEVER be reproduced without written authorization from CIISD.

Domestic Transmission Standards (Outside of Facility)

Top Secret

- Documents must be double enveloped (gum sealed, heavy duty) and sealed with government approved security tape.
- A self-addressed receipt is enclosed in the inner envelope or wrapping and the inner envelope or wrapping is closed with an approved security tape.
- Inner envelope or wrapping must bear the security marking and the recipient's address.
- Shipment must be recorded prior to leaving a Security Zone and the recipient must be notified in advance of shipment.
- Documents are sent via a security-cleared/reliability-checked individual employed by the dispatching/receiving Facility Security Cleared Canadian organization.

Secret, Confidential, and Protected "C"

- Documents must be double enveloped (gum sealed, heavy duty) and sealed with government approved security tape.
- A self-addressed receipt is enclosed in the inner

envelope or wrapping and the inner envelope or wrapping is closed with an approved security tape.

- Inner envelope or wrapping must bear the security marking and the recipient's address.
- Via:
 - a. Priority courier
 - b. Registered mail
 - c. A security-cleared/reliability-checked individual employed by the dispatching/receiving Facility Security Cleared Canadian organization

Protected "A" and "B"

- Single, gum-sealed, heavy duty envelope
- Via:
 - a. First class mail
 - b. An individual employed with the organization
 - c. Classified/Protected "C" methods

International Transmission Standards

Top Secret, Secret, Confidential, and Protected "C"

- Double enveloped (gum sealed, heavy duty) and sealed with government approved security tape
- Via CIISD

Protected "B"

- Single, gum sealed, heavy-duty envelope
- Via CIISD

Protected "A"

- Single, gum sealed, heavy-duty envelope
- Via first class mail, priority courier, or registered mail

Destruction

Unless otherwise specified, TOP SECRET, and PROTECTED "C" information and assets must be returned to CIISD for disposal.

Unless otherwise specified, SECRET, CONFIDENTIAL, and PROTECTED "A" and "B" information and assets of Canadian origin may be destroyed by the organization with the approval of CIISD.

CLASSIFIED and PROTECTED information and assets which have been authorized for destruction must be disposed of in accordance with the following:

- It must be destroyed only by approved destruction equipment, or at a facility authorized by CIISD.
- Information awaiting destruction or in transit to destruction must be safeguarded in the manner prescribed for the most highly CLASSIFIED and PROTECTED information asset involved.
- CLASSIFIED and PROTECTED information/assets awaiting destruction must be kept separate from other information/assets awaiting destruction.
- An employee with a proper security clearance or with Reliability Status, as applicable, must be present to monitor the destruction of CLASSIFIED and PROTECTED information, respectively.
- Surplus copies and waste that could reveal CLASSIFIED and PROTECTED information must be protected to the appropriate level and should be promptly destroyed.

Information System Security

The ISM establishes operational standards in Canadian industry for the safeguarding of Government information electronically processed, stored, or transmitted. This also applies to the safeguarding of technology assets. The administrative, organizational, physical, and personnel security standards as documented in the ISM also apply to the information technology environment.

The Government Security Policy requires that the degree of safeguarding provided by industry be commensurate with the level of the information and assets and the associated threats and risks. The contracting authority is responsible for ensuring that the requirements of the Government Security Policy are met and that the security standards are applied by the private sector contractor. The security standards contained in the Government Security Policy, Information Technology Standards, are the minimum standards for security in the private sector. Assessments, advice, and guidance regarding these standards are available from the Canadian and International Industrial Services Directorate (CIISD) of Public Works and Government Services Canada (PWGSC).

The prime contractor's Information Technology Facility(s) must be approved by CIISD prior to processing government information.

Conclusions

“It’s important to be responsible here and to be particularly careful after 9/11 that we’re not giving our enemies information or materials that would make their job easier.” (Chui, 2003)

John H. Marburger III,
Director, Office of Science & Technology Policy
(and science adviser to President George W. Bush)

To no surprise, the anthrax letter attacks of 2001 led directly to national policy changes since they specifically targeted both lawmakers and media personnel at their workplaces. To better protect their citizens, the United States and Canadian governments established controls not only over the possession and use of hazardous biological agents, but also over the information pertaining to their possession and use. Legislation is now in place that forbids the disclosure of information that may identify which biological agents are possessed, who possesses that agent(s) and where, and any safeguard and security measures used to protect unauthorized access to the agent(s). Because of the genuine threat of bioterrorism, biodefense research has become a vital and necessary component of an overall national security program. The United States alone has committed billions of dollars towards biodefense research and development. To protect biodefense information and assets, organizations working on projects deemed to be “classified” (for the sake of national security) must follow precise requirements, restrictions, and safeguards established by their federal government. For Canada and the United States, these requirements are conveyed in the *Canadian Industrial Security Manual (ISM)* and the U.S. *National Industrial Security Program Operating Manual (NISPOM)*. These manuals provide guidance in implementing a uni-

form and cost-effective security system, thus allowing an organization to focus mainly on research rather than the burden of developing and implementing security procedures. Without these standards and consistent security policies and practices the potential for compromise leading to a serious national security threat is enormous.

References

- Canadian and International Industrial Security Directorate. (2004). *Industrial security manual*. Available at www.ciisd.gc.ca/ism/text/preface-e.asp. Accessed online 2004.
- Chui, G. (2003). Security concerns imperil research: Restrictions shackle scientists, some say. *The Mercury News*, March 3, 2003. Available at www.mercurynews.com/mld/mercurynews/news/5303757.htm?1c. Accessed online 2004.
- Defense Technical Information Center. (2004). *National industrial security program operating manual (DoD 5220.22-M)*. Available at www.dtic.mil/whs/directives/corres/html/522022m.htm. Accessed online 2004.
- Parliament of Canada. (2004). *Public Safety Act, 2002*. Available at www.parl.gc.ca/37/3/parlbus/chambus/house/bills/summaries/c7-e.pdf. Accessed online 2004.
- U.S. Government Printing Office. (2004). *Public Health Security and Bioterrorism Preparedness and Response Act of 2002*. Available at frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ188.107.pdf. Accessed online 2004.