Critical Infrastructure Protection (CIP) Training Program

The world is rapidly changing. Our critical infrastructure is at risk on many fronts. Key services that were once taken for granted are now being affected by terrorist attacks, severe weather and other hazards that place our society and economy at risk. The systems and networks that make up the infrastructure of society are often taken for granted; yet a disruption to any one of those systems can have dire consequences across other sectors.

The earthquake and tsunami in Japan in 2011 highlighted the interdependent nature of critical infrastructure sectors, even affecting global supply chains. The disruption caused by Hurricane Katrina and the 9/11 attacks also affected several critical infrastructure sectors in the United States, regionally, and in some cases, nationally. These included communications, transportation and finance. When the 1998 Ice Storm brought down the power grid in Central Canada and the Northeastern United States, the subsequent power failures had a cascading effect on other critical infrastructure sectors.

Our dependence on information technology presents increasing vulnerabilities to critical infrastructure. The loss of the availability of computerized controls and communications systems that monitor and manage our nation's electric power grid, water supply systems, and manufacturing and financial systems can hurt the economy and endanger lives. Hence, critical infrastructure protection is a growing part of many organizations' risk management.

This unique CIP and resilience program is made up of Program, Technical, and Applied courses and instills in the students an "all-hazards" approach in assessing and managing risks that could lead to disruption in service. It also teaches students how to evaluate the ability of an organization to rapidly respond to an incident, and quickly recover operations and service delivery.

CIP Course	Course Structure
Program Course	**1.1 Introduction to CIP** Learning Objectives: the scope of Critical Infrastructure (CI) and Critical Infrastructure Protection (CIP); CIP concepts and principles; CI information and information sharing; CI stakeholders and sectors; the CIP Risk Management Model; challenges for CIP. **1.2 Resilience** Learning Objectives: Concept and scope of resilience; Resilience criteria; Infrastructure, organizational and operational resilience; Resilience strategy and planning. **1.3 Interdependencies** Learning Objectives: Concept and scope of interdependency; How interdependencies link systems; Types of interdependency failures; Notion of CI Sector Interdependencies, Proxies and Contagions; International and Corporate CI Interdependencies; Assessing Interdependency. **1.4 CIP and Business Continuity Planning (BCP)** Learning Objectives: Concept and Scope of BCP; Business Continuity Planning (BCP)

Process; Business Impact Analysis (BIA); Disruption Scenario(s); Recovery Strategy/Strategies and Teams; Relationship of BCP to CIP; BCP Standards.

1.5 CIP in an Asset Protection Organization

Learning Objectives: the relationship between CIP and other asset protection programs; the functions of the various asset protection specialties; and, CIP as a result of an effective, integrated security program.

1.6 CIP Policies

Learning Objectives: Key events that have influenced North American CIP Policy; all hazards and risk management approach to CIP; CIP policy planning environment and hierarchy; legislation and national policy related to CIP; national CIP strategy and plans; CIP collaboration and information sharing.

1.7 Mission Analysis

Learning Objectives: Concepts and Definitions of Mission Analysis; Identification of an organization's mission; Identification of key assets required for success of the mission; Mission and CIP implications.

2.1 Criticality Analysis

Learning Objectives: Identify mission critical assets using existing methodologies; Describe mission-critical assets; Rank mission critical assets using tools such as CARVER and MSHARPP.

2.2 Threat Assessment

Learning Objectives: Types of threats and hazards; All hazards approach to CIP; Threat Assessment methodologies; Intelligence Preparation of the Environment; Threat/hazard information sources; Threat levels and CI design; the relationship between threat, vulnerability and risk.

2.3 Threats and Hazards

Learning Objectives: Types of deliberate threats and threat agents; Types of environmental (natural and health) hazards; Types of occupational (accidental) hazards

2.4 Environment and Sustainable Development

Learning Objectives: The causes and effects of environmental hazards and their influence on CI; the role of interdependence and the choices of mitigation measures available for the protection and resilience of CI; how sustainable development can contribute to overall resilience and protection of CI.

2.5 Mission Analysis and Criticality Assessment Exercises

Learning Objectives: reinforce comprehension of the materials:

From Chapter 1.7: Applying mission analysis in a CIP assessment

From Chapter 2.1: Conducting a criticality assessment using the CARVER tool

2.6 Vulnerability Assessment

Learning Objectives: Definition of vulnerability and vulnerability assessment; Attributes of vulnerability; Why a vulnerability assessment is required; Vulnerability assessment methodologies and sources of information; Conduct of a vulnerability assessment; Link of vulnerability to other phases of the CIP Model.

2.7 Risk Assessment and Risk Management

Learning Objectives: Key concepts and terminology of risk the purpose of a Risk Assessment in CIP; how to conduct a CIP Risk Assessment; the benefits of Risk

Assessments in support of CI programs; the purpose of Risk Management in CIP; who is responsible for Risk Management; Risk Management strategies and techniques; Risk mitigation controls; Residual risk.

2.8 Response and Recovery

Learning Objectives: Key concepts and terminology of response and recovery; Role of Emergency Services in CIP; Components/Functions of Emergency Management; Emergency Operations Centres (EOC); Phases of Response and Recovery.

3.1 Network Analysis and Nodal Mapping

Learning Objectives: Basic concepts of Network Analysis; Construction of a network; Networks and CI; Types of CI networks; Vulnerability and protection of CI nodes and links; What Nodal Mapping is; Basic concepts of Nodal Mapping; Use of Network Mapping in CIP.

3.2 Operational Requirements

Learning Objectives: What an Operational Requirement (OR) is; why Operational Requirements are needed; who needs them; what they should include; how they should be written (content); how they should be briefed to management.

3.3 Design, Delivery, and System Integration

Learning Objectives: Design and Threat; Design and Protection; Influence of the Cost of Business in CIP; Influence of the Cost-Benefit Analysis in CIP; Influence of Value Engineering in CIP; Benefits of System Integration to CIP; CIP concerns in the Delivery, Construction or Build phases.

3.4 Planning and Management of CIP

Learning Objectives: Planning and Management of a CIP program: Planning – Strategy, Policy and Goals; Organizing - Establishing, developing, implementing and maintaining an effective CIP program; Staffing – Specification, Training and Awareness; Leading – Management, Governance and Oversight of the CIP Program; Controlling – Standards, Audit and Verification.

3.5 Threat and Risk Assessment Exercises

Learning Objectives: reinforce comprehension of the materials:

From Chapter 2.2: Threat Assessment

From Chapter 2.7: Risk Assessment and Risk Management

3.6 Project Management in a CIP Environment

Learning Objectives: Project Management (PM) principles and their application to CIP in order to improve CIP management processes through better understanding of: Planning and estimating, communication, risk management, project control and resource management. Key areas of focus are: PM Framework; PM Knowledge Areas; PM Process Groups; Application of PM to CIP.

3.7 Legal Aspects in CIP

Learning Objectives: The federal legal landscape that affects CI; Standard types of law and their purposes; Criminal law and CIP; Significant federal legislation pertaining to CIP; Regulatory requirements pertaining to CI; International Law; the law in a risk management framework.

3.8 Ethics for CIP Professionals

Learning Objectives: Concepts and key definitions of ethics; Ethical frameworks; Application of ethics; Ethics in a risk management framework; the business case for

	ethics; CII Code of Ethics; Ethics Case Study. **4.1 Government Sector** Learning Objectives: Scope of the Canadian and US Government Sectors; the approaches taken by the Canadian and US governments to protect CI that they own and operate; the approaches taken by the Canadian and US governments to assist private sector CIP; the scope and critical infrastructure issues of the Canadian and US postal sectors/sub-sectors. **4.2 Communications and Information Technology Sector** Learning Objectives: Scope and capabilities of the Communications and Information Technology (IT) Sector; Structure of the sector; Sector specific assets, threats, vulnerabilities, interdependencies, risks and safeguards. **4.3 Energy and Utilities Sector** Learning Objectives: Key definitions and concepts of the Energy Sector; Structure of the Energy Sector; Sector specific assets, threats, vulnerabilities, interdependencies, risks and safeguards. **4.4 Finance Sector** Learning Objectives: Key characteristics of the Finance Sector; Finance Sector structure and governance; Sector specific assets, threats, vulnerabilities, interdependencies, risks and safeguards. **4.5 Transportation Sector** Learning Objectives: Scope of the transportation system; Transportation modes and architecture; Sector specific assets, threats, vulnerabilities, interdependencies, risks and safeguards. **4.6 Health Care and Safety Sectors** Learning Objectives: Scope of the Health Care and Safety Sectors; the hierarchy of agencies involved in health care, safety and emergency services; Sector specific assets, threats, vulnerabilities, risks and safeguards. **4.7 Food and Water Sectors** Learning Objectives: Scope of the Food and Water Sectors; Food Sector critical assets, threats, vulnerabilities, interdependencies, risks and safeguards; Water Sector critical assets, threats, vulnerabilities, interdependencies, risks and safeguards. **4.8 Manufacturing Sector** Learning Objectives: Scope of the Manufacturing Sector; Key concepts including the supply chain; Defence Industrial Base and Chemical sub-sectors; Sector-specific threats, vulnerabilities, interdependencies, risks and safeguards.
Technical	**1.1 Mission Analysis** Learning Objective: Mission Analysis; Business Continuity Planning (BCP); Network Analysis and Nodal Mapping; Criticality Assessment. **1.2 Resilience** Learning Objectives: Resilience criteria and effects; CIP Risk Management Model and Resilience; Use of Threat Assessment, Vulnerability Assessment and Risk Assessment in identification and assessment of resilience; Use of tools in planning resilience measures; Use of Emergency Management Process in identification and assessment of resilience.

1.3 Intelligence Preparation of the Environment

Learning Objectives: Understand the complexities of the operational environment and the nature of the threat; Define the Intelligence Preparation of the Operational Environment process, its scope and its steps; Define the operational environment that is of interest to CI; Describe the effects of threats and hazards on the operational environment; Evaluate the threat to determine a Threat Level; Determine threat Courses of Action.

1.4 All Sources Research and Analysis

Learning Objectives: Definition of all source intelligence and its various sources; Intelligence Cycle; where to find all source intelligence; how to use an all hazards approach and prioritize threat information; how to create a Threat Dashboard; Key challenges for all source analysts.

1.5 Introduction to Terrorism and Sabotage

Learning Objectives: Understand: why groups use terrorism; what is a terrorist group is; how terrorist groups conduct operations; where terrorist groups are likely to strike; what sabotage is and how it is enacted; how to protect CI against acts of terrorism and sabotage.

1.6 Weapons Effects – Blast and Kinetic

Learning Objectives: Introduction to Blast and Blast/Structures Interactions; Introduction to Kinetic Weapons and how they are a threat to Critical Infrastructure.

1.7 Event Effects – Environmental and Accidents

Learning Objectives: Understand the types of natural disasters, health hazards, and accidental hazards.

1.8 All Source Threat Assessment

Learning Objectives: Learn to Assess Threats and: Collate (Prioritize) Threat Information; Evaluate (Grade/Rate) Threat Information; Analyze Threat Information; Interpret Threat Information; Disseminate (Distribute/Brief) Threat Information.

2.1 Threat Assessment Exercise

Learning Objectives: reinforce comprehension of the materials:

From Chapter 1.3: IPOE

From Chapter 1.8: All Source Threat Assessment

2.2 Security Fundamentals

Learning Objectives: Principles of Security; Security concepts; Security Safeguards; Integrated and Layered Defence; Relevance of Security Terminology.

2.3 Integrated Perimeter Security (Security of Approaches)

Learning Objectives: Integrated Perimeter Security; Physical Security and Safety of Personnel; Assessment of Approaches; Vehicle Borne Threats; Site Assessment; Vehicle Dynamics; Principles of Hostile Vehicle Mitigation; Traffic Management and Calming; Landscaping and Streetscaping.

2.4 Integrated Perimeter Security (CCTV and Lighting)

Learning Objectives: Principles of Integrated Perimeter Security Controls - Closed Circuit TV (CCTV) and Lighting Systems: Identifying the Requirement; Concepts and Design; Advantages and Disadvantages; Control Procedures; Integration Criteria.

2.5 Integrated Perimeter Security (Surveillance and Detection)

Learning Objectives: Principles of Integrated Perimeter Security Controls - Surveillance

and Perimeter Intrusion Detection Systems (PIDS): Concepts and Design; Advantages and Disadvantages; Control Procedures; Integration Criteria.

2.6 Integrated Perimeter Security (Fencing, Barriers and Access Controls)

Learning Objectives: Principles of Integrated Perimeter Security - Fencing, Barriers and Access Controls: Concepts and Design; Advantages and Disadvantages; Control Procedures; Integration Criteria; Integration of Perimeter Security Measures.

2.7 Physical Protection I

Learning Objectives: Principles of Security; Synergy of Security Effort; Hierarchical Security; Corporate Security Management ("Scheme of Manoeuvre"); Application of Layered Security (Physical).

2.8 Physical Protection II

Learning Objectives: Application of 3-D Security (Dispersion, Duplication and Deception); Application of Blast and Ballistic Resilience.

3.1 Physical Protection Exercise

Learning Objectives: reinforce comprehension of the materials:

From Chapter 2.7: Physical Protection I

From Chapter 2.8: Physical Protection II

3.2 Personnel Protection

Learning Objectives: Espionage, Sabotage, Assassination, Kidnapping; Personnel Vulnerabilities; Increasing Organizational resilience through Education: Anti-Terrorist Force Protection (AT/FP) and Operational Security (OPSEC); Human Resource Vetting: Insider Compromise, Background Investigations and Internal checks; Education Programs: Subversion and Espionage Directed Against (SAEDA), OPSEC, AT/FP, and Cyber Security.

3.3 Geographic Considerations and Site Selection/Assessment

Learning Objectives: Understand the geographic assessment methodology needed to conduct an assessment of most CI sites. This will include the application of: desk-top research, IPOE, geology, hydrology, meteorology and topography.

3.4 Building Design Characteristics and Assessment

Learning Objectives: Basic building design considerations for resilience and robustness; Structural engineering design considerations for resistance to blast loading; Architectural and operational issues that may affect structural design of CI; Design features that may be considered to enhance resilience and robustness of CI structures; Engineering inputs into the vulnerability assessment of CI.

3.5 Infrastructure Engineering

Learning Objectives: Critical infrastructure aspects of utilities including: water, HVACR, electricity supply, fuel supply, and telecommunications; major vulnerabilities and dependencies of each of these and the main mitigation measures used; role of the infrastructure engineer in a critical infrastructure assessment.

3.6 Introduction to Emergency Management

Learning Objectives: Emergency Management definitions; Emergency Management Planning; Response activities; Recovery activities; Assessment of Emergency Management Capability.

3.7 Emergency Management Planning

Learning Objectives: Purpose of Planning; Planning Cycle; Steps in the Planning

	Process; Components of a Basic Plan. **3.8 ICS, UCS, and EOC Operations** Learning Objectives: Emergency Operations Center (EOC) Roles and Responsibilities; EOC Considerations; The Incident Command System (ICS) and Unified Command (UC) Models; EOCs, ICS and CIP. **4.1 Emergency Management Exercise** Learning Objectives: : reinforce comprehension of the materials: From Chapter 3.6: Introduction to Emergency Management From Chapter 3.7: Emergency Management Planning From Chapter 3.8: ICS, UCS, and EOC Operations **4.2 Information Security Threats and Vulnerabilities** Learning Objectives: Nature and impact of cyber attacks; Threat categories /classification; Cyber attack triangle: threats, vulnerabilities, and exploits; Hacker methodologies; Attack vectors; Evolution of the cybercrime community; Emerging threats. **4.3 Information Security Protective Measures** Learning Objectives: Core concepts in information security; Major principles of information security; Information security standards. **4.4 Command and Control Systems** Learning Objectives: Basics of control systems; Nodal mapping & Network analysis; Computer command and control systems; Human command and control systems; the decision making cycle; C4ISR systems; Command and control vulnerabilities; Use of nodal mapping by attackers. **4.5 SCADA Systems** Learning Objectives: SCADA systems and their uses; differences between business IT systems and SCADA systems; IT security measures; where to find applicable SCADA security standards and guidance documents. **4.6 Trials, Testing and Evaluation** Learning Objectives: Purpose of trials, testing and evaluation; Trials and critical infrastructure protection; Types of trials; Defining the requirement for trials, testing and evaluation; Direction, management and conduct of trials; Using results of trials, testing and evaluation; Use of Computer Simulation for evaluation. **4.7 Conducting a CIP Assessment** Learning Objectives: The steps and processes in preparing for a CIP Assessment; the steps and processes in conducting a CIP Assessment; the steps and activities required after the completion of a CIP Assessment. **4.8 CIP Assessment Team Member Functions** Learning Objectives: CIP Assessment Team composition, their functions and interrelationships for each of the following team members: Team Leader, Situational Awareness Specialist, Security Operations Specialist, Engineering Specialist, Information Protection (IP) / Information Security (IS) Specialist, Emergency Management Specialist, Health and Safety/HAZMAT/CBRN Specialist.
Applied	**Introduction** This is a five-day practicum that will serve to confirm the knowledge gained from the

	Program and Technical courses. The CIP Assessment conducted is a professional assessment that will provide a real risk assessment and recommendations to the hosting facility. **Day 1 - Review of Program and Technical Courses** The review of the program and technical courses will be complemented by a sector specific overview, an introduction to the Hotwash and Murder Board process, and preparatory meetings and briefings with the instructor cadre and host facility management. **Day 2 - Day 5 - Conduct of the CIP Assessment** Instructors and candidates will conduct the assessment and will prepare the Outbrief and Executive Summary of the assessment findings. One candidate will be selected to prepare and deliver an oral presentation during the Outbrief to the host facility management.

The Program and Technical courses are delivered on-line through an effective e-Learning portal. Both are pre-requisite self-study, leading to a live facility CIP assessment as part of the practical Applied portion of the course. Each on-line course represents approximately 60 hours of study, and the practical Applied course is a five-day live facility assessment. Successful completion will result in a Professional Development Certificate attesting to the successful completion of all three courses. Alternately, classroom courses can be delivered to government and corporate clients.

Accredited through the Register for Security Engineering Specialists (RSES) in the United Kingdom (UK), this program is recognized in 16 countries as the "Gold Standard" in critical infrastructure resilience training http://www.ice.org.uk/rgn8. It exposes professionals with experience in one or more security domains, such as business continuity planning, emergency management, or personal security, to an integrated protection approach that helps clients attain a higher level of operational resilience. RSES is sponsored by the Centre for the Protection of National Infrastructure (CPNI) and is administered and operated by the Institution of Civil Engineers (ICE).

For more information and pricing regarding our CIP Training Program, please visit our website at: www.ci-institute.com.

Michel Anglehart
President
Critical Infrastructure Institute