



BASTION SECURITY
"YOUR Best Line of Defense"

Bastion Security Overview

This document is intended for “**Public**” viewing and may be disseminated freely.

The purpose of this document is to provide a general overview of the structure, operations and objectives of Bastion Security. It can be viewed as an initial introduction to the company and high-risk security in general. The intended audiences are potential clients, distributors, partners, contractors/employees, suppliers and effectively anybody with an interest in High-Risk security services and products who needs to understand our approach to High-risk / Remote Site security. More detailed information on each chapter is available, upon request, from the author of this document, or by contacting Bastion Security using the contact information at the bottom of each page of this document.

The information provided in this document is current as of the revision date shown below and is the property and original creation of Bastion Security.

Author: Douglas Konzuk - Director of Security Operations

Creation date: 15 May, 2004

Revision Date: 18 October, 2006

Summary

Bastion Security provides innovative, effective and efficient Services and Products to clients that are both in the Security Industry or the end-user and whose chief concern is results.

Objective

To provide effective protection to clients with assets operating in high-risk situations and/or remote locations globally.

Effective protection is achieved by efficiently using methods and resources which directly, or indirectly;

- *maintain the structural integrity* of the threatened asset;
- *allow the normal operations* of the client (and the assets it owns and/or controls) to continue with minimal disruptions due to security concerns;
- *minimize loss of net worth*, and
- *allow the client and its assets to meet their objectives* in a timely manner.

The key to providing effective protection is to *identify, assess and predict* the various threats and their targets **in advance** of an attack in the probable, possible and emergency response scenarios which can be expected to occur over the lifetime of the client's presence in high-risk situations and remote sites. Only *then* can the required resources and methods be identified, prepared and deployed where required, when required.

Core Competencies

To ensure the highest quality of service to its clients, Bastion Security is structured to operate within high-risk situations (includes conflict and post-conflict zones) and remote sites and has focused its talents on the following security elements;

- Security Operation Management;
- Asset Protection, including any combination of the following asset types;
 - ◆ Fixed Assets;
 - ◆ Portable Assets;
 - ◆ Human Assets, and
 - ◆ Intellectual Assets.
- Security Intelligence;
- Consulting;
- Training, and
- Security Operation Service Support.

Bastion Security takes a low-profile, modular and scalable approach to high-risk security. The underlying concept of all products and services provided is that they need to adapt to the most probable, possible and emergency response scenarios which have been identified, assessed and predicted over the life of the security task. They must be flexible enough to quickly respond, and adapt, to a changing situation as well as those which elements which have not been identified, assessed, or predicted. Most importantly, security measures should not draw attention to the client from threats which are seeking targets.

Security Services

High-Risk security has the potential to be very resource-intensive, in terms of personnel, equipment and time, if not approached in a modular and scalable manner. Effective security does not necessarily need to be expensive, but it needs to be innovative, well thought out, planned in advance, and executed effectively to be cost efficient. The structure of the Security Team deployed will be based on the protection requirements of those critical assets identified by the client, security, as well as the various threats to the client, and is flexible enough to accommodate operations of any size, scale, and scope under one command structure fully supported by the Regional Centre responsible for that operation.

The modular and scalable approach allows the insertion of additional security elements when they are required as the threat level, or the scale of the client operations, increases beyond the current ability of the security teams to provide effective protection. If this increase is temporary, the added elements can be removed once the threat level, or the scale returns to “normal” (the state that existed prior to the increase). This modular and scalable approach provides a very cost and resource efficient method of providing effective protection in the present and future.

Security Products

In conjunction with Glacis Technologies and the Business Intelligence arm of the Fortress Group of Companies, Bastion Security can provide the following products for distribution, or to enhance your existing security measures;

- Armour Kits;
- Communications Kits;
- Direct Support Kits, and
- Security Intelligence reports.

Experience

Threats within high-risk / conflict zones are generally of a higher calibre and may be prepared to pay a higher price to achieve success. That price may include personal injury to themselves, their Target, the Security Teams which separate the two, as well as innocent bystanders. Hi-Risk or Remote-Site security needs to be well planned, well executed and demands personnel which have the training, experience and mental capacity to allow them to formulate plans which minimize the interaction between the Threat and the Target. Most importantly, they must have the thought process and training which allows them to react quickly and properly to a Threat that does manifest itself.

Personnel deployed on security operations are selected from the Security Roster according to the client's requirements, employed on a contract basis, and trained as a team prior to deployment to ensure team cohesion and high standards are maintained. The necessary knowledge, skill and experience required to perform each task will vary according to the specifics of the mission and personnel are matched and trained for the probable, possible and emergency response tasks to be performed over the expected life of the deployment. A premium is placed on personnel with international experience, primarily military with at least one deployment with a UN, or NATO, peacekeeping operation, or a multi-national Humanitarian Assistance / Disaster Relief mission.

For further information on Bastion Security, a detailed overview of Bastion Security titled **Bastion Security Overview** is available in electronic form on the website, or by e-mail, or in printed form by request. Further information on each section (as titled above), is also available on the website, by e-mail, or in printed form by request.

Table of Contents

<i>Chapter</i>	<i>Section</i>	<i>Page Number</i>
Summary		i
Introduction		1
	Corporate Structure	1
Core Competencies		3
	Security Operations Management	3
	Asset Protection	3
	Security Intelligence	4
	Consulting	4
	Training	4
	Security Operations Service Support	4
Security Services		5
	Management Tasks	5
	Asset Protection Tasks	5
	Security Intelligence Tasks	6
	Consulting Tasks	6
	Training Tasks	6
	Service Support Tasks	6
Security Products		7
	Armour Kits	7
	Communications Kits	7
	Direct Support Kits	7
Experience – Key Contact		8
	Key Contact	8
	CV Summary	9

Introduction

Bastion Security provides innovative, effective and efficient Services and Products to clients that are both in the Security Industry or the end-user and whose chief concern is results.

Objective

To provide effective protection to clients with assets operating in high-risk situations and/or remote locations globally.

Effective protection is achieved by efficiently using methods and resources which directly, or indirectly;

- *maintain the structural integrity* of the threatened asset;
- *allow the normal operations* of the client (and the assets it owns and/or controls) to continue with minimal disruptions due to security concerns;
- *minimize loss of net worth*, and
- *allow the client and its assets to meet their objectives* in a timely manner.

The key to providing effective protection is to *identify, assess and predict* the various threats and their targets **in advance** of an attack in the probable, possible and emergency response scenarios which can be expected to occur over the lifetime of the client's presence in high-risk situations and remote sites. Only *then* can the required resources and methods be identified, prepared and deployed where required, when required.

Corporate Structure

To fully understand how security operations are planned and conducted by Bastion Security, irregardless of location, size, task or client, it is necessary to introduce how both the company and its operations are structured and how an operation is approached anywhere in the world. Due to the inherent risk in providing security in high-risk situations and/or remote locations where local police or security forces can not be depended on to provide effective protection, Bastion Security has been modelled on a military command structure and mindset and operations are approached in a similar manner to United Nations Peacekeeping missions. The personnel must be capable of working in very stressful and potentially dangerous situations, in conflict or post-conflict zones, where the threats and/or their targets are military or paramilitary in nature.

As with a UN peacekeeping mission, it is preferred that negotiation and peaceful resolution to conflict occur. However, where the threats or targets are military or paramilitary (terrorist, rebel, guerrilla forces, etc) the security team must have the knowledge, skill, experience and resources to avoid, deter or negate these threats prior to a successful attack on the client's assets. Most importantly, the command and control elements which are present in these situations and intimately involved must be allowed to use their initiative and judgement to react to or anticipate threats with full confidence that their actions will be supported by their superiors. This involves trust of their abilities and the assurance that the team leaders and members are highly trained and well equipped. Effective protection can not be provided if all required elements are not predicted and provided at the right place in advance of their being needed. There is rarely a second chance in these situations.

Every attempt is made to operate Bastion Security as a business entity with minimal overhead, in order to keep expenses and client charges to a minimum. To ensure this is accomplished, the permanent corporate command and control as well as support infrastructure is kept to a minimum and only expanded as necessary. To this end, there are three distinct levels to Bastion Security, each with their duties and responsibilities;

- Corporate Headquarters;
- Regional Centre, and
- Country Office.

Corporate Headquarters

The primary function of the Corporate Headquarters is company growth, primarily through the creation, and support of Regional Centres. Support is provided by providing direction, coordinating effort, creating and implementing doctrine and the creation of the corporate intelligence database. The database provides the basic background intelligence necessary to perform security operations in high-risk locations around the world. Other tasks of the Corporate Headquarters include specialized Consulting services which are not effectively employed at each Regional Centre.

The Corporate Headquarters for Bastion Security is presently co-located with the Corporate Headquarters of The Fortress Group of Companies Ltd, on the outskirts of Calgary, Alberta, Canada. Bastion Security is a member of the Fortress Group of Companies Ltd.

Regional Centre

The primary function of the Regional Centre is to coordinate and provide support to all clients (of both products and services) within the geographical regions of that Region. As the company expands and requires a permanent local presence to better support clients around the world, new Regional Centres will be created, under Bastion Security Corporate ownership. Regional Centres will be designated in two manners, as follows;

- Minimal. A newly created regional centre will only have the command and control (Regional Executive and Management) personnel and minimum support infrastructure on a permanent basis. The necessary staff and infrastructure required to support country offices and clients (services and products) will generally be utilized on a contract basis, as necessary. A minimal regional centre may be created on a temporary basis to support a number of short-term clients, or may be the first step to establishing a permanent presence in that region and allows corporate operations to be performed while suitable local staff, property and external support organizations are identified and secured.
- Full. Geographical regions which have the necessary client base to support a permanent presence there will merit a full regional centre, which will be fully staffed primarily by permanent Bastion Security personnel and have a permanent infrastructure to support clients across the full range of core competencies.

The structure, duties and responsibilities will be similar across all Regional Centres, (minimal or full) with particular emphasis on intelligence and training support. As a default, the main Regional Centre is responsible for all client operations until such time as a new Regional Centre is dedicated to that geographic territory. All client requests for products and services will be directed to, and be handled by, the applicable Regional Centre which is responsible for the client's geographical location. At the present time, the default Regional Centre is co-located with the Corporate Headquarters of Bastion Security.

Country Office

If sufficient client support is required in a specific country, or local regulations require a local presence or national staff to perform any business transactions, then a country office will be created to support all client requests for security products and services within that country. The country office may have corporate ownership, or be owned and operated by local business people under a franchise agreement. Where no country office exists, all client interactions will typically take place with the Regional Centre.

Core Competencies

Bastion Security provides services and products to individuals and organizations operating in high-risk situations and remote sites globally with the objective of providing **effective protection** while utilizing client and security resources in an efficient manner. In order to meet this objective, all aspects of security operations must be studied and understood, and thus it is essential that your security provider have knowledge, skill and experience in all the necessary aspects of security.

The system created by Bastion Security is designed for one purpose: *To detect and identify threats and predict their targets in **advance** of an attack in order to provide sufficient warning for the protection teams to allow them to plan a course of action which will ensure that the resources required to **effectively** avoid, deter or negate that threat are made available at the required time, in the required location.*

A detailed study of high-risk security illustrates that there exists six distinct elements which must be considered and implemented through the appropriate combination of security services and products. Those six elements are described in the following sections.

<i>Primary</i>	<i>Secondary</i>	<i>Tertiary</i>
Operations Management	Consulting	Service Support
Asset Protection	Training	
Intelligence		

Security Operations Management

Management elements of the Security resources required to provide effective protection are responsible for the following;

- Overall command and control of security resources (focus on the the big picture);
- Identification, Ranking and Classification of assets owned, or controlled by the client and key external organizations present in the situation.
- Creation and implementation of the security plan;
- Coordination of effort to ensure that all aspects of the plan are considered and performed;
- Identify, source, secure, acquire, prepare and deploy the necessary resources required to provide effective protection to the proper location, at the required time, and
- Evaluate and assess performance of all components present during security operations and apply lesson's learnt to future operations.

Security Intelligence

Accurate and timely intelligence forms the basis of the security plan and advanced warning of probable or long-term known Threats is essential to provide all elements of the Security Team with adequate time to plan an effective course of action which will avoid, deter or negate the Threat. This process is renewed on a continual basis, not only to ensure the threat model is consistent with current conditions, but also to identify those conditions which must change to create new threats, or can be changed to negate these current Threats.

Of a secondary nature, but no less important, is the need to deny information (or provide mis-information) to the various threats which have targeted assets of the client and are in the planning or execution stages of *their* operation. These Counter-Intelligence Duties are vital to reducing the chances of a successful attack against the Client or Security teams.

Asset Protection

Protection services and products are designed to provide **effective** protection of the following asset types against a wide range of threats;

- fixed assets (including fixtures, structures, open areas, facilities, etc.);
- portable assets (including objects, containers, vehicles, convoys, etc.);
- human assets (ranging in scale from individuals to groups, crowds and events, etc.), and
- intellectual assets (various types of information including ideas, plans, policies, etc.)

Consulting

Consulting Products and Services are utilized to create, analyze, and critique the implementation of, the security plan. Of particular interest are its strengths, weaknesses and relevance with respect to the current and potential threats. Their focus is on providing an objective look at the key players present within the situation to ensure that effective protection is achievable and the vulnerabilities of each are assessed, investigated and either corrected, or exploited as suitable.

Training

Security training has two distinct components which have a completely different audience and intent;

- Formal. Aimed at the security professional who is, or can expect to be, operating in high-risk situations and remote locations anywhere in the world. Their aim to increase the depth and breadth of knowledge of Security personnel to ensure they are masters of their craft and able to operate effectively in the most hostile environments and fluid situations.
- Informal. Aimed at client personnel who are, or will be, operating in High-Risk areas, or Remote sites, and have no formal security training, or experience. Informal training transfers basic knowledge, skills and experience which will allow them to assist security personnel, thus increasing their effectiveness. The resulting knowledge, skills and experience is not sufficient to perform the duties and responsibilities of the various elements of the Security Team, but greatly **reduces** the chances that they will become a Target.

An educated client is essential to achieving effective protection and incurs lower costs due to security as the resources required are decreased in comparison to one with no *street smarts*, so to speak.

Security Operations Service Support

Support requirements of any task or operation may be necessary to ensure that the required infrastructure, equipment and supplies, logistic and administrative concerns are addressed and actioned;

- Operations Support (including Communications, Interpreters, local guides, medical, and other support required to ensure operations can be performed);
- Logistical Support (including transport, accommodations, rations, maintenance, and other support required to ensure that the proper resources are available where required, when required), and
- Administrative Support (including financial, records, library and other support required to ensure that proper records are properly kept and allows the various security elements to perform their duties, instead of getting bogged down in the paperwork.

For a more information on this chapter, please consult the document titled **Core Competencies Summary** which is available electronically (.html and .pdf format) on the website, by e-mail (.pdf format), or on paper by request, or by contacting us directly by phone.

Security Services

Security operations utilize an intelligence-led approach to predict under which conditions potential threats will manifest themselves and against which targets, allowing effective deployment of Security Teams. High Risk security operations can only be effective when the Protection Teams have adequate time to formulate plans to counter the expected and probable threats. Mutual support by Bastion Security Teams *increases* the effectiveness of the main protection force by providing **advanced warning** of predicted, unknown or random threats and provides a quick reaction to enhance protection in the event of surprise or random threats.

Bastion Security Operations are designed to be quick-reaction and every effort is made to reduce the deployment time to an absolute minimum without sacrificing operational readiness and effectiveness. For this reason, and due to the vast scope of Security Operations and the skills required, a roster based approach to staffing exists. Security Team members and leaders will be chosen from the roster in accordance with the skills and training required for the particular operation. Extensive military training and experience in International operations within a United Nations, NATO, or (multi)national command structure is typical in the roster.

Depending on the specifics of the security operation, any combination of security teams may be deployed, as required, to provide effective protection, or augment existing security teams. The modular nature of the Security Teams allow them to be inserted (or removed when their tasks are finished) into existing security operations, whether they are performed exclusively by Bastion Security, or are controlled by in-house, or external, security forces and utilize Bastion Security Teams to increase their effectiveness.

Security Operation Management Tasks

Management Teams provide the necessary leadership for an effective operation and is responsible for the overall command of the operation. The focus is on the big picture and has the aim of ensuring that all aspects of the Security Plan are considered and executed. A management team is essential for large, complex or geographically diverse operations as it allows the various elements of the Security Team to concentrate on their specific tasks. This is accomplished by ensuring the proper resources are sourced and readied in advance of being required, and are utilized effectively once incorporated into the Security Plan. The primary task of the Management Team is the identification, classification and ranking of potential targets. Targetted assets are not only those which are essential to their owners, but also those which are identified as being of high value or importance to the Threats. The Management Team also acts as liaison between the Client and Security to ensure recommendations or concerns voiced by either party are addressed and acted on.

Asset Protection Tasks

Protection Teams are concerned with the (in)direct protection of those Targets designated as primary, which are those at highest risk of an attack from immediate or known Threats. They are *reactionary* by nature and rely on a high level of training and mutual support from other teams to ensure that they are able to effectively protect themselves and the targets in the event of an attack. The Protection Team is the most visible, if not the only visible, element of the Security Team. Their presence or actions may help to deter any threat from manifesting against the target in question. Protection Tasks rely heavily on Direct Support and Intelligence Teams to provide advanced warning of Threats and allow the Protection Team additional time to plan a course of action which will avoid, deter or negate the Threats prior to an attack. Support Teams increase the geographic influence of the Protection Team by preceding mobile targets along a route to its destination(s) to ensure they are secure or safe for travel, or by detecting the presence of threats which are planning or executing an attack on a static or mobile target. The Support Team also provides additional protection layers in response to an increase of the threat level and when the situation requires. Support Teams also act as a Rapid Reaction Force (RRF) to provide backup if the threat level escalates beyond the capability of the Protection Team or an attack manifests itself against the Primary Target.

Intelligence Tasks

The Intelligence Team is the Early-Warning System for any security operation. Its primary task is the identification, classification and ranking of potential threats to the Security Team. Accurate and timely intelligence forms the basis of the security plan and advanced warning of probable or long-term known Threats is essential to provide all elements of the Security Team with adequate time to plan an effective course of action which will avoid, deter or negate the Threat. This process is renewed on a continual basis, not only to ensure the threat model is consistent with current conditions, but also to identify those conditions which must change to create new threats, or change the ranking of the existing threats. Secondary tasks of the Intelligence Team focus on denying information on the Client and Security structure, operations and objectives to potential threats while still in their planning phase.

Consulting Tasks

Consulting Teams are utilized to create, analyze, and critique the implementation of, the security plan. Of particular interest are its strengths, weaknesses and relevance with respect to the current and potential threats. Assessment, Investigation and Special Function tasks can be performed, as required, to support existing security operations.

Training Tasks

Their primary tasking is to increase the depth and breadth of knowledge of Bastion Security personnel to ensure they are masters of their craft and able to operate effectively in the most hostile environments and fluid situations. They can be utilized in any phase of the operation to ensure the Security Teams have the skills to meet the Threats likely to be encountered in addition to being kept up to date with new technologies or tactics being utilized. Training Teams are also available to provide standard or custom training courses in a wide variety of security subjects to security teams external to Bastion Security.

Management, employees and contractors of the Client can also benefit from shorter, less detailed informal courses or seminars by being made aware of what their responsibilities are during a security operation. This can range from simple common sense matters such as why security is present and their impact on the operations and daily routine and what to do if a Threat does manifest itself, to training in escape and evasion / survival skills and self-defence in accordance with the Threat level and wishes of the Client.

Security Operation Service Support Tasks

The duties and composition of the Support Task Force will be dictated by the operational effectiveness, logistical, and administrative support requirements of the Operation. They may be necessary to ensure that the required infrastructure, equipment and supplies, logistic and administrative concerns are addressed and actioned.

For a more information on this chapter, please consult the document titled **Security Services Summary** which is available electronically (.html and .pdf format) on the website, by e-mail (.pdf format), or on paper by request, or by contacting us directly by phone. Contact information is available below.

Security Products

Products designed for Bastion Security follow the same general principles as the services Bastion provides. Above all, they increase the effectiveness of the Security Teams present. The design philosophy of our products is to complement, not replace, the security personnel required to provide effective protection of your assets with an efficient utilization of client and security resources.

These products are designed to demanding specifications to ensure they will function properly in the harshest environments, such as conflict zones. In keeping with the design philosophy, all kits are created with the user in mind, whether they be a security professional, or any individual / organization operating in high-risk situations and remote sites anywhere in the world.

Armour Kits

Bastion Security armour kits are designed and manufactured to provide protection against ballistic threats. These threats are usually caused by explosives (shrapnel), or high-velocity projectiles (bullets). The portable and temporary nature of these kits makes them ideal for organizations which do not require ballistic protection of their assets permanently (24 hours a day, 7 days a week), or rent/lease equipment, vehicles, and structures (fixed or portable) and thus are not able to apply permanent armour to these asset types, but still need their contents protected from ballistic threats. The portable nature allows the armour to be stored and transported by personnel, or vehicle, with ease and minimal delay.

Communications Kits

Bastion Security communications kits are designed and assembled to provide reliable and effective communications within and between all levels of those organizations operating in high-risk areas or remote sites. These kits are ideally suited for organizations operating in high-risk or remote sites on a temporary basis and do not wish to deploy a fixed communications system and all the associated support infrastructure or where local supply or the necessary infrastructure and support structure does not exist, or is not reliable.

Direct Support Kits

Identifying real or potential threats and providing advanced warning of these threats to the asset protection teams is essential to providing effective protection in high-risk situations and remote sites. As the size and scale of the security operation increases, the manpower requirements to effectively observe all sectors within the site and surrounding area increases dramatically. Bastion direct support kits are designed to assist the protection elements of the security teams and are ideally suited for organizations with a temporary presence in a location, or are operating in areas where it is not suitable to install fixed systems, or quality components are not available in sufficient quantity in the task area.

Please note that the range of products to be offered will expand significantly in the near future to cover the full range of the core competencies of Bastion Security. This document will be expanded to cover these new products as they become available for general sale, or distribution.

For a more information on this chapter, please consult the document titled **Security Products Summary** which is available electronically (.html and .pdf format) on the website, by e-mail (.pdf format), or on paper by request, or by contacting us directly by phone. Contact information is available below.

Experience - Key Contact

Bastion Security Operations are designed to be quick-response and every effort is made to reduce the deployment time to an absolute minimum. For this reason, and due to the vast scope of Security Operations and the skills required, a roster based approach to staffing exists. Security Team members and leaders will be chosen from the roster in accordance with the skills and training required for the particular operation. External announcements for operational deployment will only be made if a complete Security Team can not be filled from the roster. Employment contracts, irregardless of length, will include pre-deployment, deployment and post-deployment duties. Common pre-deployment duties will include, but are not limited to, operation specific; briefings, training, equipment readiness, medical, legal, logistic and administrative details. Post-Deployment duties will encompass; de-briefing, equipment maintenance, assessment, revision of Operating Procedures in light of 'Lesson's Learnt' and final reporting to client.

Personnel may be deployed in situations in which they augment existing security forces which may be commanded by external (in-house or contract) security forces. Deployment in these situations may be for a specific task or to provide a specific skill which is not currently available in the existing security force. The ability to adapt and adhere to different operational methods, management styles or local customs is essential. Considerable responsibility is delegated to field personnel at all levels as Team Members may be working alone or in small groups without direct supervision from Team Leaders or Management at any time.

For further information about the knowledge, skills and experience required for inclusion on the Security roster, please consult the document titled **Security Team Roster Summary** which is available electronically (.html and .pdf format) on the website, by e-mail (.pdf format), or on paper by request, or by contacting us directly by phone. Contact information is available below.

Key Contact - Douglas Konzuk (Director of Security Operations)

For further information about our services, approach to security operations, please visit our web page at the address listed below. Please feel free to contact me, by e-mail or telephone, either to discuss your situation, or arrange a meeting to obtain further details about securing our products and services. As Director of Security Operations, I am your key contact within Bastion Security and I look forward to working with you personally to ensure the safety and security of you, your organization and those people and external organizations who depend on you. Attached is a summary of my personal CV to indicate my security knowledge, skill and experience. Personnel selected for security contracts of all types will have similar or complementary skills and training.

CV Summary – Douglas Konzuk CD,BSc

Personal Information

Personal Strengths

Leadership	Experience	Pressure / Stress	Planning
-------------------	-------------------	--------------------------	-----------------

Experience

	<i>Military / Intelligence / Security</i>	<i>Business</i>
Total:	19 years	10 years
International:	4 years	4 years
International Residency:	3 years	1 years

Medals / Commendations

Military medals have been awarded for the following;

- United Nations Mission in Cyprus (UNFICYP)
- United Nations Mission in the Former Republic of Yugoslavia (UNPROFOR)
- Humanitarian Mission to East Africa (Special Service Medal with *Humanitarian Bar*)
- Canadian Peacekeeping Service Medal
- Canadian Forces Decoration (CD) which is awarded for 12 years of distinguished service

A "wound stripe" was awarded as a result of injuries sustained from an anti-tank land mine while on active service in the Former Republic of Yugoslavia. Was also nominated for the **Meritorious Service Medal** while on active service in the Former Republic of Yugoslavia.

Education / Training

Formal

University of Toronto (Canada) – BSc (Astronomy and Physics)
 University of Calgary (Canada) – various courses taken for professional development.

Military Courses – Student

<i>General</i>	<i>Leadership</i>	<i>Intelligence</i>	<i>Infantry</i>
Basic / Recruit	Junior Leadership	Combat Intelligence	Basic and Advanced Infantry
Driver – Wheeled Vehicles	Senior Leadership		Machine Gunner
Small Arms Coach			Infantry Section Commander
Basic Parachutist			
Military Motorcycle Driver			

Military Courses – Instructor

<i>General</i>	<i>Leadership</i>	<i>Infantry</i>
Basic / Recruit	Basic Officer Training	Basic and Advanced Infantry
Driver – Wheeled Vehicles	Combat Leadership	Reconnaissance
Driver – Armoured Vehicles		Infantry Section Commander

Security Courses – Student

Basic Security Guard	Body Language and Questioning Techniques	Criminal Tactics
Surveillance	Technical Surveillance Counter-Measures	Undercover Operations
Counter – Surveillance	Evaluating Questioned Documents and Suspicious Paperwork	Situational Awareness
Surveillance Photography	Explosive Device Detection	Security Investigations
Labour Disputes / Strikes	Counter – Terrorism Driving	Self-Defence (Unarmed)
Executive Protection	Security Alarms and Counter-Intrusion	Security Consulting
Firearms (Armed Guard)		

Security Courses – Instructor

Body Language and Questioning Techniques
--

Military Employment

<i>Unit</i>	<i>Position</i>	<i>International Deployment</i>	<i>Primary Duties</i>
1 PPCLI (Infantry)	Section Commander	UNPROFOR – Yugoslavia DART – East Africa	Intelligence Collection Protection and Security
G&SF (Infantry)	Platoon Second in Command	NATO Exercise – Norway NATO Exercise – Germany UNFICYP – Cyprus	Infantry Section 2IC Heavy Weapons Commander Reconnaissance

Security Employment

<i>Company</i>	<i>Position</i>	<i>Primary Duties</i>
Bastion Security	Director of Security Operations	Overall command and control of Security Operations
Mitchell and Associates	Private Investigator	All aspects of fraud and criminal investigations
North Group Intl.	Protection Team Leader	All aspects of Close (Personal) Protection operations.
Intercon Security	Protective Services Operative	Mobile Patrol / Alarm Response.
United Nations (MONUC)	Security Officer (Professional)	Create and run new Security Intelligence Unit.

Note: Security employment does not include tasks performed through Bastion Security, only those positions held as an employee of external organizations.

A detailed overview of this Curriculum Vitae is available on request.