IROC Phase II

Concept of Operations/Location Study

CONFIDENTIAL

Threat Risk Assessment and Recommendations Report

Prepared by:

Enterprise Protection Associates

Kimley-Horn and Associates, Inc.

September 10, 2007

091845004

Copyright © 2007, Kimley-Horn and Associates, Inc.

TABLE OF CONTENTS

Threat Risk Assessment and Recommendations Report

1. EXECUTIVE SUMMARY 1

2. PROJECT DEFINITION 2

3. INTRODUCTION, BACKGROUND, AND METHODOLOGY 3

3.1 Introduction 3
3.2 Methodology 3

4. FACILITY CHARACTERIZATION AND CANDIDATE LOCATION 4

5. MISSION CRITICAL ASSETS 5

5.1 Findings 6

6. THREATS, RISKS AND HAZARDS 6

6.1 State Crime Trends 6
6.2 CAP Index Report 12
6.3 Terrorism and Extremism 19
6.4 Organized Crime 20
6.5 Criminal Networks 20
6.6 Opportunity Crime 21
6.7 Insider Crime 21
6.8 Criminal Attack Vectors 22
6.9 Wild Fire 23
6.10 Natural Disaster 24
6.11 Traffic 24
6.12 Sabotage 25
6.13 Cyber Crime 25
6.14 Workplace Violence 26
6.15 Catastrophic Events Involving Weapons of Mass Destruction 26
6.16 Findings 29

7. RISK EQUATION 30

7.1 Target Attractiveness 30
7.2 Consequence Evaluation 33
7.3 Deterrence 34
7.4 Threat 34
7.5 Calculations of Risk 35

8. VULNERABILITIES 35

8.1 Characterizing the Security Requirement 36
8.1.1 Public Access 37
8.1.2 Motor Vehicles 37
8.1.3 Parking 38

TABLE OF CONTENTS

Threat Risk Assessment and Recommendations Report

8.1.4 Internal Access ... 39
8.1.5 Local-Area Network/Wide-Area Network ... 39
8.1.6 Secure Collocate Facility ... 39
8.1.7 Communications ... 39
8.1.8 Meeting and Conference Rooms ... 39
8.1.9 Common Spaces ... 39
8.1.10 Emergency Power and Fuel Storage ... 39
8.1.11 Communication Antennas ... 40
8.1.12 Mail and Courier Traffic ... 40
8.1.13 Critical Dependencies ... 40

9. RECOMMENDATIONS ... 40

9.1 Physical Security ... 41
9.1.1 Buffer Zones ... 41
9.1.2 Stand Off Distance ... 42
9.1.3 Perimeter Demarcation ... 42
9.1.4 Gates ... 43
9.1.5 Interior Roadways ... 43
9.1.6 Lighting ... 44
9.1.7 Crime Prevention Through Environmental Design ... 44
9.1.8 Signage ... 45
9.1.9 Building Surfaces ... 45
9.1.10 Doors Types ... 46
9.1.11 Door Frames ... 46
9.1.12 Hinges ... 47
9.1.13 Locking Hardware ... 47

9.2 Security Systems ... 48
9.2.1 Integration ... 48
9.2.2 Access Control System ... 49
9.2.3 Intrusion Detection and Alarm System ... 50
9.2.4 Closed-Circuit Television System ... 50

9.3 Security Policy and Procedures ... 55
9.3.1 Background Checks ... 56
9.3.2 Photo Identification Badging ... 56
9.3.3 Key and Access Card Control ... 57
9.3.4 Deprovisioning ... 57
9.3.5 Contractors ... 57
9.3.6 Visitors ... 58
9.3.7 Access and Pedestrian Traffic Flow ... 58
9.3.8 Incident Reporting ... 58
9.3.9 Records Management ... 59
9.3.10 Change Control ... 59
9.3.11 Security Awareness Training ... 59
9.3.12 Systems Training ... 61
9.3.13 Performance Measurement ... 61
9.3.14 Security Continuity of Operations ... 61

TABLE OF CONTENTS

Threat Risk Assessment and Recommendations Report

9.3.15 Security System Monitoring 62
9.4 Preventative Maintenance 64

10. SUMMARY OF RECOMMENDATIONS AND FINDINGS 65
10.1 Findings 65
10.2 Strategic Recommendations 66
10.3 Tactical Recommendations 67

LIST OF TABLES

Table 1 – Offense by Category 9
Table 2 – Offense by Location 10
Table 3 – Local Crime Trends 11
Table 4 – Methods and Consequences of Attack 23

LIST OF ACRONYMS

ACHD	Ada County Highway Department
ACS	Access Control System
CCTV	Closed-Circuit Television
CDC	Center for Disease Control
CPTED	Crime Prevention Through Environmental Design
DHS	Department of Homeland Security
DVMS	Digital Video Management System
DVR	Digital Video Recorder
EMS	Emergency Medical Services
EPA	Enterprise Protection Associates
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FHWA	Federal Highway Administration
GIS	Geographic Information System
HVAC	Heating, Ventilation, and Air Conditioning
IDS	Intrusion Detection System
IED	Improvised Explosive Device
IO	Information Operations
IP	Internet Protocol
IPP	Infrastructure Protection Program
IROC	Interagency Regional Operations Center
ISP	Idaho State Police
IT	Information Technology
ITD	Idaho Transportation Department
PTZ	Pan/Tilt/Zoom
TMC	Traffic Management Center
UCR	Uniform Crime Reporting

1. EXECUTIVE SUMMARY

Organizations face significant security challenges in today's world where protecting vital assets can be an expensive and daunting proposition. Meeting the security challenge for the Interagency Regional Operations Center (IROC) in Meridian, Idaho requires new thinking; a new model for security management that weaves the different elements that protect your assets into a single, complete and easily managed solution. The new security management model aligns security with business needs by integrating three critical components in the security environment: user management, facility management and information management. Each component must be open and flexible, easily integrating with one another as well as with third-party solutions. Finally, security management demands a proactive approach and on-demand response to events within the ever-changing security environment. When properly implemented, security management enables the understanding of the security environment in all of its complexity, turning security data into actionable information, obtaining timely answers to critical questions and taking the appropriate action to protect the asset. A comprehensive security management plan delivers multiple benefits including reduced risk and liability exposure.

The future holds promise of ever-increasing adversarial sophistication, capability and determination. Adversarial groups are shifting from symmetrical to asymmetrical tactics and from independent to networked structures meaning that the facility's security measures must be sustainable, flexible, robust and resilient. Mandating security is an executive responsibility that requires cooperation by the leaders of all of the vested agencies. The most effective method is to create a policy that articulates the purpose, application, responsibility assignments, references and objectives of the security program and empowers all of the facility's workers in the effort to protect IROC assets.

Securing any facility and protecting its human resources and material assets requires a combination of physical, logical and electronic measures aimed at deterring, detecting and delaying an adversary so that a timely, effective and appropriate response can be mounted. Leaders too often focus on security technology while overlooking the need for security logic – internal practices that integrate security procedures with the business processes thereby fully exploiting the security technology and maximizing the return on that investment.

Security operating procedures will be needed to guide the execution of the security policy and implementation of the security measures. Each component of the security program: the physical, logical and electronic measures will require a set of procedures outlining their functions, integration and operational characteristics. The procedures will also explain how end-users will interact with each of the measures, (e.g. entering an access controlled area) and administrative requirements, (e.g. managing the card access database). Security system monitoring and event assessment protocols will be required to ensure that security events are recognized, acknowledged, and assessed quickly and assigned the correct priority prior to initiating a response. These protocols will facilitate appropriate responses, minimize the unnecessary deployment of limited resources and facilitate performance measurements.

Security response planning is also need to support the achievement of the security mission objectives. Security measures are only effective if the response leads to a satisfactory conclusion. Security responders need to understand what constitutes a satisfactory conclusion and require guidance in the form of a response plan. Response plans are event driven and take full advantage of the detection and surveillance equipment in the field to provide timely and high quality information by the monitoring agent to the responder. Modern security technology is capable of delivering detailed information in real time therefore it is unacceptable for a responder to arrive at a situation without a clear understanding of

the nature of the event, its implications to his/her safety and that of the facility and his/her role in bringing the event to a satisfactory conclusion.

The IROC must have a scaleable response plan that governs the IROC's ability to escalate and de-escalate its security measures to meet known or anticipated threat conditions. The objective is to swiftly adjust the deterrent, detection and response capabilities without unduly interfering with the facility's operational performance. Each security measure must be flexible enough to adapt to changing conditions. The IROC manager must be authorized to escalate and de-escalate the security measures according to changing conditions.

The IROC must not provide the means for an adversary to carry-out an attack. Hazardous chemicals, firearms, incendiary and explosive substances must be kept inside secure containers within the perimeter or banned from the facility all together. Management must remain vigilant to any prospect for an inside worker posing a threat to the facility resulting from personal circumstances or environmental stresses.

The project team should consider applying for funding under the Department of Homeland Security (DHS) Infrastructure Protection Program (IPP) which is designed to strengthen the Nation's ability to protect critical infrastructure facilities and systems. The IPP consists of several grant programs, including the Transit Security Grant Program. These grants fund a range of preparedness activities, including strengthening infrastructure against explosive attacks, preparedness, planning, equipment purchase, training, exercises, and security management and administration costs. The IPP programs support objectives outlined in the interim National Preparedness Goal and related national preparedness doctrine, such as the National Incident Management System, National Response Plan, and the National Infrastructure Protection Plan.

2. PROJECT DEFINITION

Enterprise Protection Associates (EPA) was tasked to perform a threat assessment to:

- Better understand the intentions and capabilities of potential adversary groups;
- Determine the attractiveness of the IROC facility as a target;
- Evaluate the overall threat potential to the IROC facility.

EPA will then assess current security conditions for the client, and provide recommendations that would lead to an appropriate security profile. The methodology consisted of four separate and distinct phases:

- *Phase I* – Asset Prioritization;
- *Phase II* – Threat Determination;
- *Phase III* – Vulnerability Assessment; and
- *Phase IV* – Gap Analysis.

3. INTRODUCTION, BACKGROUND, AND METHODOLOGY

3.1 Introduction

The term *security* is often interpreted to mean the presence of 'stuff' or people intended to guard against loss. Properly defined, security means the *condition* that exists in the absence of threats, risks, and hazards. True security is established by taking all reasonable precautions to guard against unacceptable risk. The security fundamentals are:

- Assets occupy three broad categories: infrastructure (including personnel), information, and image;
- Crime has three necessary ingredients: motive, means and opportunity;
- Loss events are perpetrated by insiders, outsiders, or both, operating in collusion; and
- Appropriate security solutions come in three forms: physical, logical, and electronic measures.

Organized crime has successfully infiltrated some of the most 'secure' organizations and their facilities. Terrorism continues to be a cause for concern by national and international police and intelligence organizations. Some of the most talented individuals in the game of espionage have migrated from former Soviet Bloc countries to North America. A recent discovery resulting from investigations conducted by law enforcement and intelligence agencies and independent security investigators revealed evidence of networking between transnational terrorist and organized crime groups. The risks to Information Technology (IT) resources are many, varied and often complex: fraud, theft, denial of service, internal mischief, snooping, hacking, spoofing, server shutdown, data and web-site forgery, viruses, mail bombs, brute force attack, and impersonation to name just a few.

A crime can be perpetrated by either 'insiders' and 'outsiders' or both, operating in collusion, meaning that the assets are not just exposed to an external attack but to an attack initiated or supported by someone who has an intimate relationship with the any of the participating agencies. Research conducted annually by the Federal Bureau of Investigation (FBI) reveals that upwards of 70 percent of corporate loss events are perpetrated by insiders.

Fire is usually a greater and more probable threat than crime. Modern communications and data centers undergo enormous pressure during crisis events. Fires inside these types of facilities are caused by electrical faults in raceways, cable trays, beneath raised floors, and inside other concealed areas. Fire can also be caused by arson, sabotage, power surges, and lightning strikes. Due to the high concentration of personnel and communication assets within IROC, fire prevention and suppression should be given a high priority during facility design. Response and recovery plans should be formulated to reinstate normal operations as quickly as possible following a disruption.

Global, national, regional, and local conflict is on the rise; environmental conditions are in flux; sophisticated and determined adversaries exist; however, the greatest threat to security is organizational complacency.

3.2 Methodology

Our methodology included identifying the core assets to determine their criticality, assessing the known and suspected threats (both external and internal) and identifying the vulnerabilities

inherent to the facility by virtue of its mission, geographic location, design and operating characteristics and proposed security initiatives. Because the IROC project is based on a new facility, the vulnerability component is less intensive – there are no existing physical security issues to consider or upgrade. Any vulnerability will stem from internal processes for the various stakeholders. A gap analysis using these factors will enable the development of a comprehensive plan to guide the design and implementation of appropriate security measures.

The approach is divided into four phases:

- Facility Characterization and Critical Asset Identification;
- Threat Analysis;
- Vulnerability Assessment; and
- Gap Analysis (this phase will occur at a later date).

In the development of this report, the Federal Highway Administration (FHWA) *Guide to Physical Security Risk Management for Transportation Management Centers* was consulted and used as a reference point.

4. FACILITY CHARACTERIZATION AND CANDIDATE LOCATION

IROC is intended as a Transportation and Emergency Management Center to be staffed and operated by multiple stakeholders. The facility is intended to provide coordinated management of transportation information and emergency response information. The benefits of this approach have been detailed in previous documents on this project.

From a security perspective, the unique aspect of this project is the fact that there will be multiple users sharing one or more workspaces, each with their own particular concerns. In a corporate environment many organizations share the same security requirements; however, in this particular (non-corporate) situation the security needs of the stakeholders can be very different. The fact that the Idaho State Police (ISP) is one of the potential future participants in the project raises the security stakes for all. ISP has increased security requirements, in some measure, simply because of the nature of the work they perform; however, if another agency is to share space and access to critical assets, the security cannot be compromised to accommodate the other agencies. As a result, any security design should be taken from what could be termed a “highest common denominator” approach. In essence, what this means is that for any particular security state in a shared environment, the requirement of the most secure stakeholder should become the requirement for all.

Site selection has a very definite effect on the eventual security measures chosen. Factors that come into play in selection include neighborhood (residential, commercial, industrial), nearby emergency services, utilities, and environmental issues. Additional factors to consider would include ease of accessibility to the area by intruders, location of nearby rail or highway with hazardous materials implications, and the existence of local transportation for employees at the facility.

All of these issues should be considered when determining the appropriate facility location. If there are no police nearby to respond to security events, then security should be somewhat stronger, providing a greater delay function to the intruder. If there is no access to secondary power sources, then generators should be kept on-site to keep the facility operating in the case of emergencies.

5. MISSION CRITICAL ASSETS

The vision of IROC is to "Create an Interagency Regional Operations Center to enhance the coordination and collaboration among the region's transportation and public safety organizations." The IROC will be a multi-discipline facility intended to accommodate key transportation and emergency service agencies, each performing important functions with varying degrees of integration, and internal and external dependencies. As a result, there will be some shared resources as well as shared risk associated with agency interdependence on resources.

Assets exist in three broad categories: infrastructure, information, and image.

The infrastructure category includes the building (or buildings), property and equipment, as well as the human resource and information technology components. These are the things that are essential to ongoing service delivery. The information category includes print records, electronic data, and media storage devices. The image category includes all things associated with the organization's reputation and its ability to maintain the public trust.

Asset criticality is determined by measuring the degree of influence the loss of the asset would have on the organization or the community it serves:

High Criticality – Any asset or combination of assets that are identified as critical to the achievement of organizational objectives, the loss of which would seriously impair the organization's ability to achieve its mission requirements or potentially compromise public health and safety.

- Appropriate measures include: access controls, detection, assessment and response protocols, Emergency, Business Continuity and Disaster Recovery Plans, system redundancy, inventory re-supply and mutual aid agreements, and a media liaison and communications strategy.

Moderately Critical – Any asset or combination of assets that are identified as important to the achievement of the organizational objectives, the loss of which would adversely impact the organization's ability to meet its mission requirements, but would not create a risk to public health and safety.

- Appropriate measures include: An emergency preparedness plan and re-supply and mutual aid agreements.

Low Criticality – Any asset or combination of assets that are identified as non-critical, the loss of which would not create a risk to public health and safety and would not require immediate re-supply or replacement.

- Appropriate measures include: physical security and mutual aid agreements.

Maintaining the safety and security of human resources will always remain the highest consideration. The physical plant (building) and its construction elements are important, but not as important as the human resources. Because a principal business driver is the sharing, integration, and coordination of information, the assets needed for gathering, distributing, analyzing, and disseminating information are also a prime consideration. These include computer hardware and software, data servers, network components, and communications devices and processes.

Given the facility's mission, the command, control, and communications infrastructure (e.g., cabling, power supplies, and heating, ventilation, and air conditioning [HVAC]) is vital. Public utility

interconnects that supply the facility with power, water, gas, sewer, and telecommunications services also will be important to the facility's operation, particularly during crises or protracted events.

5.1 Findings

Interviews with the various stakeholders brought about a general consensus in terms of asset criticality. Without exception, the responses indicated that personnel were the most critical asset, followed by equipment and communications infrastructure on-site.

The value, sensitivity, and criticality of the assets under protection at this facility means that IROC should be treated as a high-security venue.

6. THREATS, RISKS AND HAZARDS

6.1 State Crime Trends

Since 1974, Idaho has participated in the National Uniform Crime Reporting (UCR) Program, a nationwide statistical collaboration designed to collect accurate crime data from all law enforcement agencies in a "uniform" manner. The program's primary objective is to provide a reliable set of criminal statistics for law enforcement purposes. Law enforcement administrators can utilize these statistics for operational use, such as determination of manpower and training needs, proper focus of enforcement efforts and deterrence programs, budgets, and grant proposals. Furthermore, these statistics can provide valuable information to assist law enforcement in identifying specific crime activity facing law enforcement. The National UCR Program is administered by the FBI. Crime reporting on the national level is currently accepted under two methods: summary based and incident based.

Idaho law enforcement agencies report only under the incident based reporting method. In compliance with Idaho Code 67-3006 and 67-2915, the ISP and fellow law enforcement agencies throughout Idaho submit crime data under the Idaho UCR Program. Crime data, reported by 105 Idaho law enforcement agencies, represents 99.8 percent of the population of Idaho for the year 2005. Statewide rates are calculated on an adjusted population base of 1,425,914.

The incident based method collects the following: Group "A" offenses and arrests data, which includes an additional 22 crime categories in conjunction with Part 1 crime; arrest data only on Group "B" offenses. The data presented herein was obtained from the *Crime in Idaho* 2005 Uniform Crime Report.

Group "A" Offenses			Group "B" Offenses (reported only when an arrest is made)
Crimes Against Persons	**Crimes Against Property**	**Crimes Against Society**	
Murder	Robbery	Drug/Narcotic Violations	Bad Checks
Negligent Manslaughter	Burglary/Breaking & Entering	Drug Equipment Violations	Curfew/Loitering/Vagrancy
Forcible Rape	Larceny/Theft Offenses*	Gambling Offenses*	Disorderly Conduct
Forcible Sodomy	Motor Vehicle Theft	Pornography	DUI
Sexual Assault w/Object	Arson	Prostitution Offenses*	Drunkenness
Forcible Fondling	Destruction of Property	Weapon Law Violations	Nonviolent Family Offenses
Aggravated Assault	Counterfeiting/Forgery		Liquor Law Violations
Simple Assault	Fraud Offenses*		Peeping Tom
Intimidation	Embezzlement		Trespass of Real Property
Kidnaping	Extortion/Blackmail		All Other Offenses
Incest	Bribery		Runaways - (not a crime, only reported when law enforcement apprehends juvenile)
Statutory Rape	Stolen Property Offenses		

Group A crime offenses numbered 91,004 during 2005, down slightly from the previous year. Property crimes accounted for 63 percent, 22 percent were crimes against persons and 15 percent represented crimes against society. The crime rate averaged 6,901 per 100,000 of population between 2001 and 2005. The rate dropped by 7.5 percent in 2005. The following *Facts at a Glance* were taken from the 2005 *Crime in Idaho* Uniform Crime Report.

Facts At A Glance

Group "A" Offenses

- 91,004 total Group "A" offenses reported.
- 4.7% decrease from 2004 Group "A" offenses.

Crime Rate*

- 6382.2 per 100,000 inhabitants based on Group "A" offenses.
- 8.5% decrease from 2004 NIBRS crime rate.
- 2927.9 per 100,000 inhabitants based on Part 1 offenses (utilized for comparison purposes with non-NIBRS states).

Violent Crime

- 3,639 violent crime offenses reported.
- 5.7% increase from 2004 violent crime offenses.
- 6.7% increase of aggravated assault offenses, which accounts for 76.1% of the violent crime.

Crimes Against Persons

- 20,169 reported crimes against persons.
- 3.1% decrease from 2004 crimes against persons.
- 4.5% decrease of simple assault offenses, which accounts for 67.2% of the total crimes against persons.

Officers Assaulted

- In 2005, no law enforcement officers were killed in the line of duty.
- 279 total assaults on Idaho law enforcement officers.
- 1.4% decrease from 2004 of reported officers assaulted.

Hate Crime

- 27 reported hate crime incidents in Idaho for 2005.
- 27% decrease from 2004 hate crimes reported.

Crimes Against Society

- 13,825 reported crimes against society.
- 4.2% decrease from 2004 society crime offenses.
- 3.0% decrease of drug/narcotic violations, which accounted for 46.8% of the total crimes against society.

Property Crime

- 57,010 reported crimes against property.
- 5.4% decrease from 2004 total property crime offenses.
- 6.9% decrease of larceny/theft offenses, which accounted for 48.1% of the total crimes against property.
- 7.4% increase in stolen property loss from 2004.

Offenses in a variety of categories are statistically presented in **Table 1**.

Table 1 – Offense by Category

Offense	Reported in 2005	Reported in 2004	Percent Change	Offenses Cleared	Percent Cleared	Percent of Category	Rate per 100,000*
Murder	41	30	36.7%	20	48.8%	0.20%	3.0
Negligent Manslaughter	5	5	0.0%	3	60.0%	0.025%	0.4
Forcible Sex Offenses:							
Forcible Rape	567	577	-1.7%	220	38.8%	2.81%	41.8
Forcible Sodomy	75	89	-15.7%	36	48.0%	0.37%	5.5
Sexual Assault with Object	43	73	-41.1%	21	48.8%	0.21%	3.2
Forcible Fondling	912	1,038	-12.1%	345	37.8%	4.52%	67.3
Aggravated Assault	2,768	2,594	6.7%	1,451	52.4%	13.72%	204.2
Simple Assault	13,553	14,192	-4.5%	7,255	53.5%	67.20%	1000.0
Intimidation	1,714	1,766	-2.9%	508	29.6%	8.50%	126.5
Kidnaping/Abduction	284	236	20.3%	94	33.1%	1.41%	21.0
Nonforcible Sex Offenses:							0.0
Incest	13	20	-35.0%	5	38.5%	0.06%	1.0
Statutory Rape	194	195	-0.5%	91	46.9%	0.96%	14.3
Crimes Against Persons Total	20,169	20,815	-3.1%	10,049	49.8%	22.16%	1488.1
Robbery	263	247	6.5%	74	28.1%	0.46%	19.4
Burglary/Breaking & Entering	7,653	7,700	-0.6%	973	12.7%	13.42%	564.6
Larceny/Theft Offenses	27,417	29,442	-6.9%	5,103	18.6%	48.09%	2022.9
Motor Vehicle Theft	2,758	2,696	2.3%	479	17.4%	4.84%	203.5
Arson	282	320	-11.9%	71	25.2%	0.49%	20.8
Destruction of Property	12,908	14,516	-11.1%	1,868	14.5%	22.64%	952.4
Counterfeit/Forgery	2,015	1,982	1.7%	502	24.9%	3.53%	148.7
Fraud Offense	2,751	2,426	13.4%	478	17.4%	4.83%	203.0
Embezzlement	284	295	-3.7%	110	38.7%	0.50%	21.0
Extortion/Blackmail	9	12	-25.0%	3	33.3%	0.02%	0.7
Bribery	1	7	-85.7%	0	0.0%	0.002%	0.1
Stolen Property Offenses	669	631	6.0%	442	66.1%	1.17%	49.4
Crimes Against Property Total	57,010	60,274	-5.4%	10,103	17.7%	62.65%	4206.3
Drug/Narcotic Violations	6,464	6,667	-3.0%	5,183	80.2%	46.76%	476.9
Drug Equipment Violations	6,009	6,329	-5.1%	4,908	81.7%	43.46%	443.4
Gambling Offenses	5	9	-44.4%	2	40.0%	0.036%	0.4
Pornography/Obscene Material	48	33	45.5%	20	41.7%	0.35%	3.5
Prostitution	8	10	-20.0%	5	62.5%	0.06%	0.6
Weapon Law Violations	1,291	1,385	-6.8%	827	64.1%	9.34%	95.3
Crimes Against Society Total	13,825	14,433	-4.2%	10,945	79.2%	15.19%	1020.0
Total Group "A" Offenses	91,004	95,522	-4.7%	31,097	34.2%		6714.4

Crime occurrences by location type are presented in **Table 2**.

Table 2 – Offense by Location

Location:	Murder	Rape	Robbery	Agg. Assault	Simple Assault	Intimi-dation	Kidnap	Burglary/ B & E	Vehicle Theft	Arson	Destruct. of Prop.	Drug Viol.
Air/Bus/Train Terminal	0	0	0	1	7	1	0	5	7	1	14	49
Bank/Savings	0	0	25	1	7	6	1	9	5	0	30	12
Bar/Night Club	1	4	8	120	564	18	2	54	39	3	184	82
Church/ Synagogue	0	0	2	5	18	4	0	52	9	5	133	7
Commercial/ Office Building	0	3	2	16	69	41	1	474	126	15	622	100
Construction Site	0	0	1	8	13	3	1	255	16	5	159	3
Convenience Store	0	0	36	19	107	19	3	63	25	0	71	96
Department Store	0	0	4	7	67	19	2	73	19	2	78	130
Medical Facility/ Hospital	1	4	4	14	109	14	0	66	4	3	84	55
Field/Woods	0	14	5	46	85	12	3	27	31	38	311	130
Government Building	0	4	0	6	78	35	2	45	9	3	206	101
Grocery Store	0	0	7	19	69	15	1	37	9	3	73	102
Highway/Street	3	24	50	402	1,029	121	48	42	308	29	1,351	6,267
Hotel/Motel	0	19	4	26	119	5	5	40	16	1	92	225
Jail/Prison	0	0	0	57	132	10	0	0	1	0	42	94
Lake/Waterway	0	0	1	10	20	3	0	5	2	0	34	28
Liquor Store	0	0	0	0	1	0	0	3	0	0	3	0
Parking Lot	0	14	7	73	323	17	3	118	279	6	779	469
Rental Storage	0	1	0	2	3	0	0	297	12	0	54	20
Residence	26	405	69	1,316	7,392	970	132	4,999	1,540	113	6,865	3,636
Restaurant	1	0	6	19	108	34	2	123	15	3	149	69
School/College	0	9	4	68	851	91	7	153	23	28	606	465
Service Station	0	0	8	14	35	8	0	24	14	0	43	32
Specialty Store	0	1	14	12	63	20	0	399	140	11	385	54
Other/Unknown	0	35	5	53	250	64	9	263	99	12	494	223

The three prime candidate locations are located in the city of Meridian, Idaho. **Table 3** illustrates local crime trends for that community.

Table 3 – Local Crime Trends

Meridian Police Department

Population: 46,118
County: Ada

Offense Overview

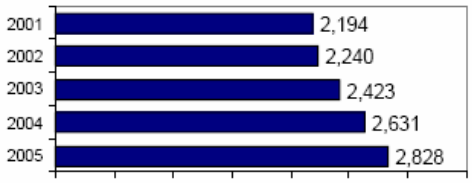
- Offense total 2,828
- % change from 2004 7.5
- # of cleared offenses 1,021
- Percent cleared 36.1
- Group "A" Crime Rate per 100,000 population 6132.1
- Summary based reporting crime rate per 100,000 population is calculated for other state crime comparisons only. 2951.1

Arrest Overview

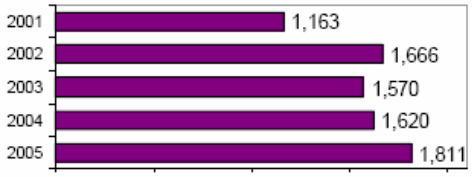
- Arrest total 1,811
- % change from 2004 11.8
- Adult arrest total 1,235
- Juvenile arrest total 576
- Arrest Rate per 100,000 population 3926.9

	Offenses		Arrests	
Group "A" Offenses	# Reported	# Cleared	Adult	Juvenile
Murder	1	1	2	0
Negligent Manslaughter	0	0	0	0
Forcible Rape	12	5	2	0
Robbery	7	1	0	1
Aggravated Assault	67	38	27	7
Burglary	254	21	15	7
Larceny	938	202	135	113
Motor Vehicle Theft	72	10	3	9
Arson	10	2	0	1
Simple Assault	355	253	138	32
Intimidation	51	27	5	3
Bribery	0	0	0	0
Counterfeiting/Forgery	106	17	9	0
Vandalism	311	43	11	23
Drug/Narcotics	179	144	111	32
Drug Equipment	174	149	70	13
Embezzlement	13	5	2	1
Extortion/Blackmail	0	0	0	0
Fraud	161	36	18	0
Gambling	0	0	0	0
Kidnaping	3	0	0	0
Pornography	2	1	0	0
Prostitution	0	0	0	0
Forcible Sodomy	9	7	0	6
Sexual Assault w/Object	6	1	0	0
Forcible Fondling	38	16	3	10
Incest	6	3	0	1
Statutory Rape	6	2	1	0
Stolen Property	24	20	17	0
Weapon Law Violation	23	17	4	2
Total Group "A"	2,828	1,021	573	261

Total Offenses - 5 year trend



Total Arrests - 5 year trend



	Arrests	
Group "B" Arrests	Adult	Juvenile
Bad Checks	2	0
Curfew/Vagrancy	0	36
Disorderly Conduct	25	5
DUI	269	9
Drunkenness	1	0
Family Offense-nonviolent	0	0
Liquor Law Violation	84	64
Peeping Tom	0	0
Runaways	0	86
Trespass	6	10
All Other Offenses	275	105
Total Group "B"	662	315

6.2 CAP Index Report

CAP Index specializes in the analysis and prediction of vulnerability to crime and is not merely a reflection of crime rates for a particular area. CAP Index analysis takes into account a wide range of geographic and demographic characteristics that dispose an area to criminal activity. There are 21 characteristics evaluated by the CAP Index model. When this data is compiled and analyzed, a picture of an area's vulnerability to crime emerges. The methodology for the model evaluates the social disorder of an area to determine the risk of different types of crime. The model accounts for factors such as:

- Population data;
- Housing data;
- Population mobility;
- Economic data; and
- Education data.

There are two elements to the report that provide useful information. The first element is the Crimecast scores. They detail the potential for a particular type of crime in a given area, compared to the potential for that crime being committed elsewhere nationally, regionally, or locally. Scores can range from 1 to 2000. A score that is equal to that for another area is expressed as 100. By example:

	National	State	County
Theft	75	100	50
Assault	500	450	300

From this example it is determined that the potential for theft to occur at the particular site is below (or 75 percent) the potential for theft nationally. The potential for theft is equal to the potential for theft elsewhere in the state, and it is below (50 percent) the potential for theft elsewhere within the County. The potential for an assault to occur at the site is higher than (by 5 times) the national potential, higher than (by 4.5 times) the state potential, and higher than (by 3 times) the local potential. We can extrapolate that the site has a higher potential for crimes against persons; however, an equal or lower potential for property crimes than areas elsewhere nationally, statewide and locally. This information aids in both security planning and the identification of appropriate asset protection measures.

The second element of the report is the map. The map is a graphic representation of CAP Index scoring for the area within which the site exists. The CAP Index score is the weighted average of the potential for crimes of violence (against persons) including homicide, sexual assault, robbery, and assault. This score is displayed as a factor of the national average (a score of 100 being equal to the national average). If the map shows the area as scoring 500, that area faces a potential for crimes of violence that is five times the national potential.

An important consideration in using the CAP Index and Crimecast reports is the tendency of crime to migrate toward opportunity. Although a particular area may be relatively safe, crime that is occurring in its surrounding area will very likely begin to spill over the area boundaries into the safer area.

The scores on the map are not specific to one crime, or in fact crime in general. They are the Index score, which is a weighted average of the risk of sexual assault, robbery, and murder. These are selected because they present the greatest personal risk to an organization or its employees. The map scores are relative to a national average of 100. A map score of 300 indicates that the risk of an indexed crime is over three times the national average for this area.

Candidate locations that were evaluated for their CAP Index score include:

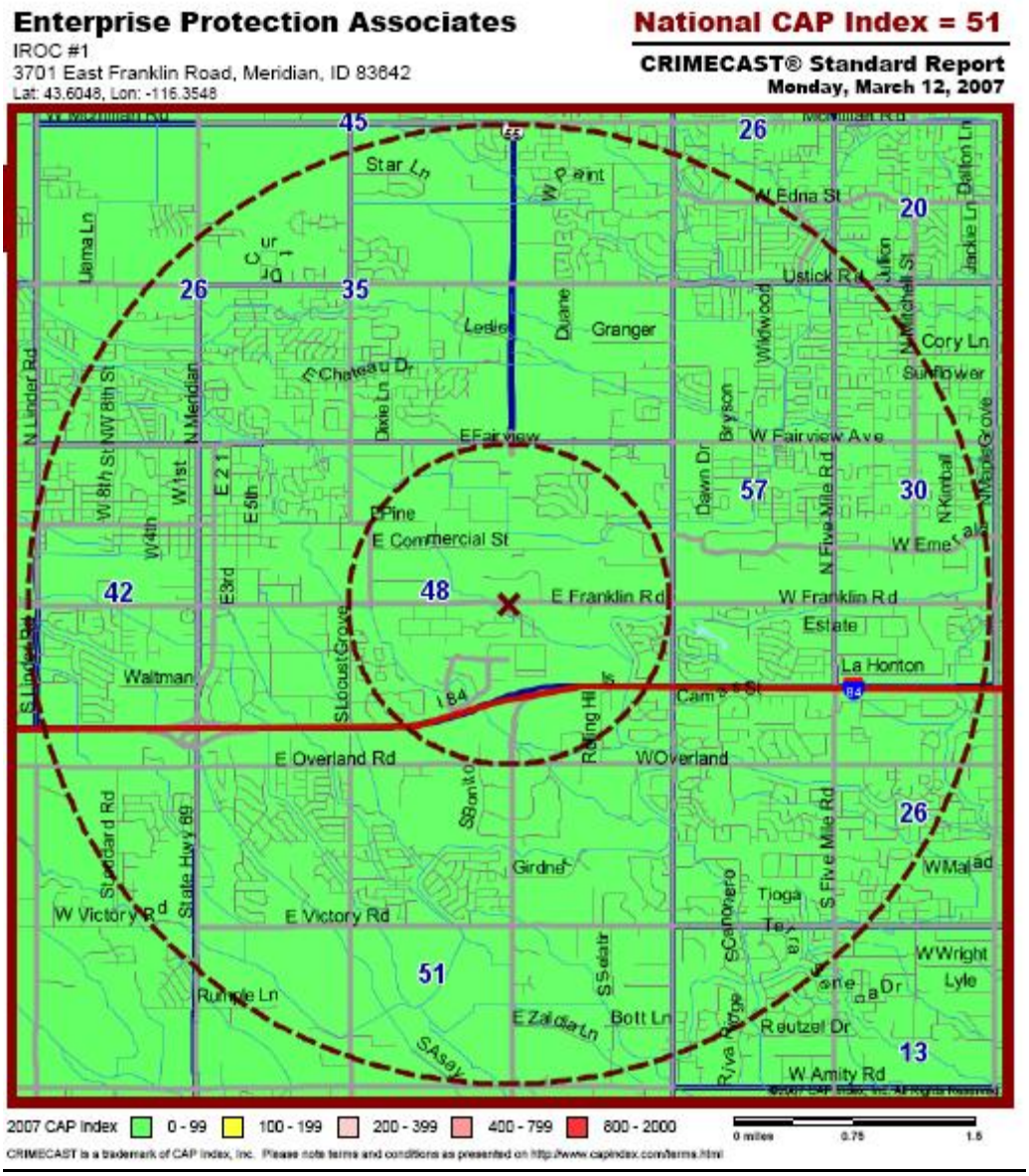
- Site 1 – Southwest corner of Franklin Road and Eagle Road;
- Site 2 – North of ISP Campus;
- Site 3 – Expand existing ISP Dispatch Center;
- Site 4 – Northwest corner of I-84 and Meridian Road; and
- Site 5 – East of ISP Campus.

Candidate locations 1, 2, 3, and 5 were near equal in their respective National CAP Index Scores of 51 and 52. Candidate location 4 had the lowest National CAP Index Score of 47. None of these scores indicate a serious and ongoing problem with serious crime.

The information gleaned from these reports indicates that compared to the National CAP Index, all three areas under consideration are well below average (see map scores); however, there are some trends that could be of concern for the potential IROC locations. Certain types of crime have indicated as above average, and the predicted future scores show a continued rise in many of these types of crime. For example, robbery relative to the county overall has risen 10 percent in the past several years in this area, and is expected to increase at about the same rate over the next five years. Property crimes show a similar trend. Fortunately, while crimes against persons have risen somewhat, it appears the increase is expected to level off over time; however, it is still higher than might be desired for people working and traveling in an area.

The following CAP Index scores are provided for Sites 1, 2, and 4. Site 3 and Site 5, which are the options of expanding the existing ISP Dispatch Center on the ISP Campus or locating IROC just east of the ISP campus, has the same boundary for crime statistics as Site 2 north of the ISP campus and therefore is already captured by the Site 2 CAP Index score.

Site 1


Enterprise Protection Associates
IROC #1
3701 East Franklin Road, Meridian, ID 83642
Lat: 43.6048, Lon: -116.3548
National CAP Index = 51
CRIMECAST® Standard Report
Monday, March 12, 2007
45
26
20
26
35
57
30
42
48
51
26
13
Star Ln
W Edna St
Ustick Rd
Leslie
Duane
Granger
Cory Ln
Sunflower
E Chateau Dr
Dixie Ln
E Fairview
W Fairview Ave
Bryson
Dawn Dr
Pine
E Commercial St
N Five Mile Rd
W Emerald
E Franklin Rd
W Franklin Rd
Estate
La Horton
Waltman
S Locust Grove
I 84
Camas St
E Overland Rd
W Overland
Girdner
Tioga
W Victory Rd
E Victory Rd
W Wright
Lyle
Rumple Ln
E Zaldia Ln
Bott Ln
Reutzel Dr
W Amity Rd
2007 CAP Index
0 - 99
100 - 199
200 - 399
400 - 799
800 - 2000
0 miles
0.75
1.5
CRIMECAST is a trademark of CAP Index, Inc. Please note terms and conditions as presented on http://www.capindex.com/terms.html

Site 1 (continued)

Site Name: IROC #1
Site Address: 3701 East Franklin Road, Meridian, ID 83642
Lat: 43.6048 Lon: -116.3548

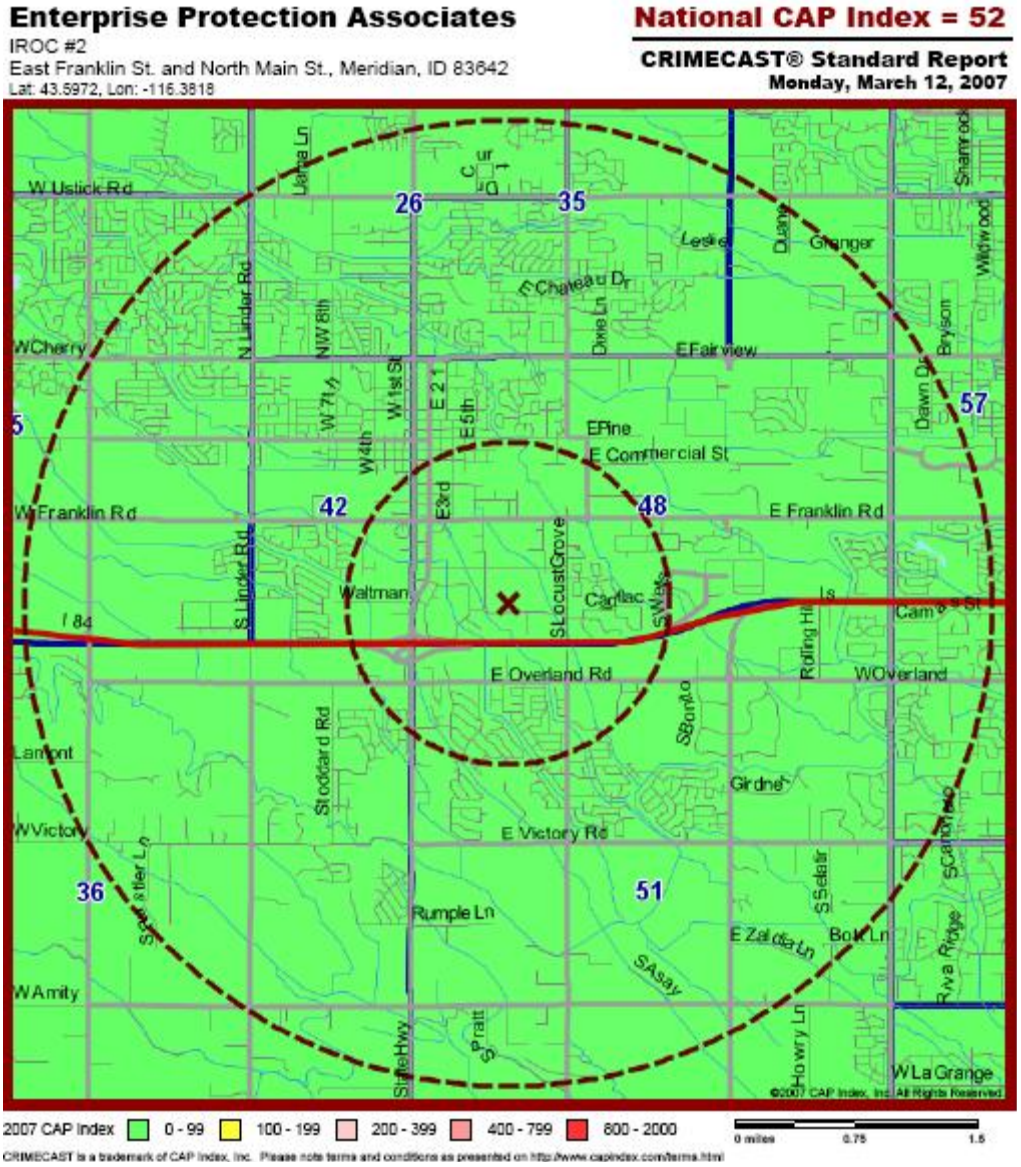
Current Scores (2007)	National Scores	State Scores	County Scores
CAP Index	51	106	103
Homicide	51	96	99
Rape	74	143	157
Robbery	51	108	102
Aggravated Assault	40	58	71
Crimes Against Persons	45	73	84
Burglary	50	75	83
Larceny	65	78	84
Motor Vehicle Theft	97	134	124
Crimes Against Property	66	84	89

Scores indicate the risk of crime at a site compared to the average of 100. (i.e. A score of 400 means that the risk is 4 times the average and a score of 50 means the risk is half the average.

Past Scores (2000)	National Scores	State Scores	County Scores
CAP Index	42	97	94
Homicide	42	88	92
Rape	59	128	141
Robbery	42	99	93
Aggravated Assault	34	54	71
Crimes Against Persons	37	67	79
Burglary	42	68	80
Larceny	59	75	80
Motor Vehicle Theft	85	130	122
Crimes Against Property	58	79	85

Future Scores (2012)	National Scores	State Scores	County Scores
CAP Index	55	108	107
Homicide	52	95	98
Rape	78	144	158
Robbery	56	112	108
Aggravated Assault	41	56	68
Crimes Against Persons	47	73	83
Burglary	53	76	84
Larceny	67	78	85
Motor Vehicle Theft	103	134	125
Crimes Against Property	69	85	91

Site 2


Enterprise Protection Associates
IROC #2
East Franklin St. and North Main St., Meridian, ID 83642
Lat: 43.5972, Lon: -116.3818
National CAP Index = 52
CRIMECAST® Standard Report
Monday, March 12, 2007
26
35
42
48
57
36
51
W Ustick Rd
W Cherry
W Franklin Rd
E Franklin Rd
E Fairview
E Pine
E Commercial St
E Overland Rd
W Overland
E Victory Rd
W Victory
W Amity
W La Grange
Rumple Ln
Waltman
Cartlac
Girdner
Leslie
Granger
Bryson
Wildwood
Shamrock
Dawn Dr
Rolling Hills
Cameo St
Lamont
Stoddard Rd
S Linder Rd
N Linder Rd
S Locust Grove
S Meridian
S Cole
S Eagle Rd
S Pratt
S Cantrell
Riva Ridge
Howry Ln
E Zaldea Ln
Bolt Ln
S Sasay
I 84
©2007 CAP Index, Inc. All Rights Reserved
2007 CAP Index 0 - 99 100 - 199 200 - 399 400 - 799 800 - 2000
0 miles 0.75 1.5
CRIMECAST is a trademark of CAP Index, Inc. Please note terms and conditions as presented on http://www.capindex.com/terms.html

Site 2 (continued)

Site Name: IROC #2
Site Address: East Franklin St. and North Main St., Meridian, ID 83642
Lat: 43.5972 Lon: -116.3818

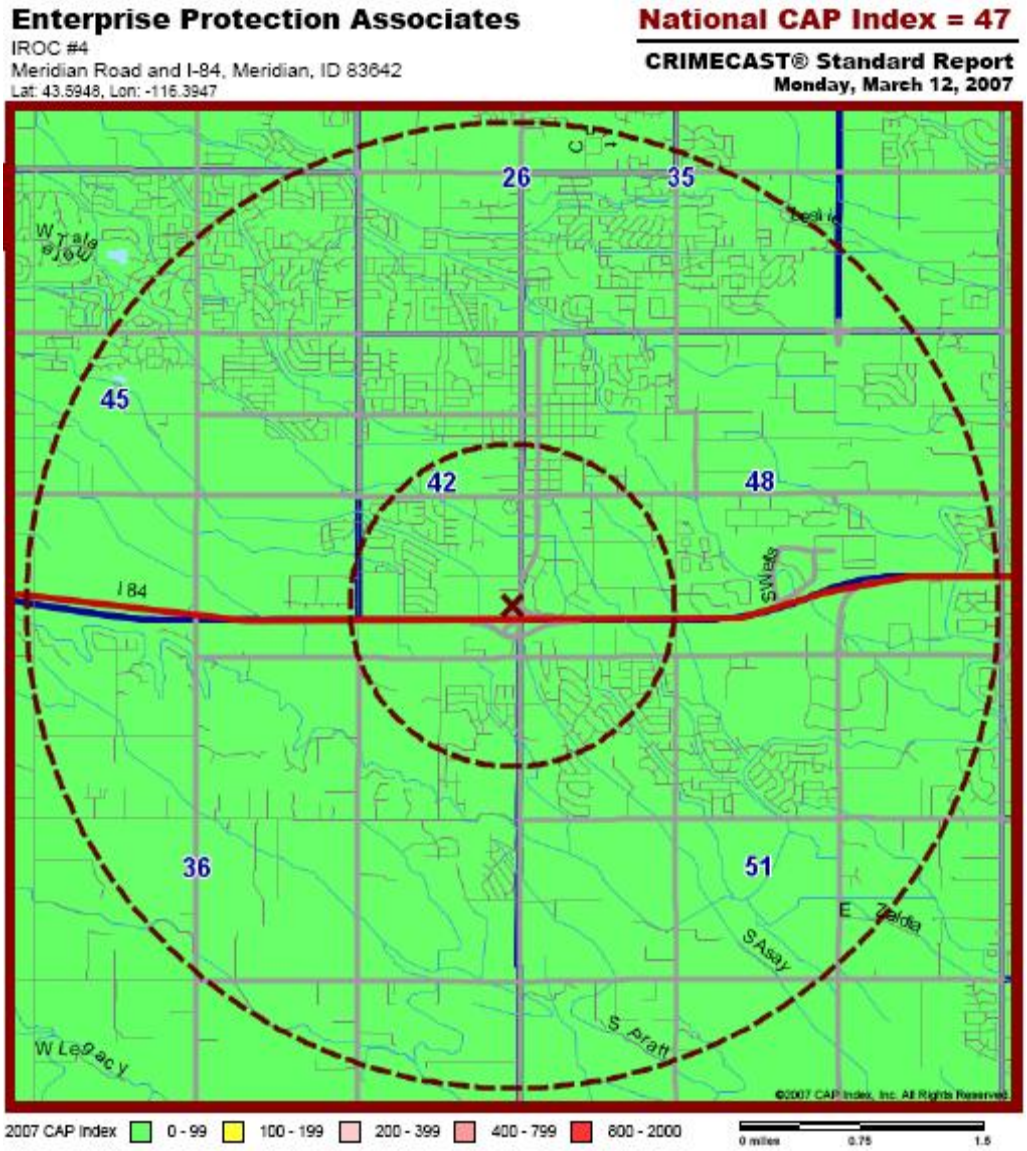
Current Scores (2007)	National Scores	State Scores	County Scores
CAP Index	52	108	105
Homicide	65	123	126
Rape	89	173	188
Robbery	48	102	96
Aggravated Assault	56	81	100
Crimes Against Persons	53	86	99
Burglary	75	112	125
Larceny	64	77	82
Motor Vehicle Theft	105	145	134
Crimes Against Property	71	90	96

Scores indicate the risk of crime at a site compared to the average of 100. (i.e. A score of 400 means that the risk is 4 times the average and a score of 50 means the risk is half the average.

Past Scores (2000)	National Scores	State Scores	County Scores
CAP Index	41	94	92
Homicide	54	111	118
Rape	70	150	167
Robbery	38	89	84
Aggravated Assault	43	88	90
Crimes Against Persons	41	74	88
Burglary	58	94	111
Larceny	55	70	75
Motor Vehicle Theft	86	132	123
Crimes Against Property	58	79	85

Future Scores (2012)	National Scores	State Scores	County Scores
CAP Index	58	110	109
Homicide	67	123	124
Rape	96	178	194
Robbery	53	106	102
Aggravated Assault	62	85	103
Crimes Against Persons	58	90	102
Burglary	82	118	130
Larceny	69	80	88
Motor Vehicle Theft	117	153	142
Crimes Against Property	77	95	101

Site 4


Enterprise Protection Associates
IROC #4
Meridian Road and I-84, Meridian, ID 83642
Lat: 43.5948, Lon: -116.3947
National CAP Index = 47
CRIMECAST® Standard Report
Monday, March 12, 2007
26
35
45
42
48
36
51
I 84
W Legacy
S Pratt
S Asay
E Zelda
©2007 CAP Index, Inc. All Rights Reserved.
2007 CAP Index
0 - 99
100 - 199
200 - 399
400 - 799
800 - 2000
0 miles
0.75
1.5

Site 4 (continued)

Site Name: IROC #4
Site Address: Meridian Road and I-84, Meridian, ID 83642
Lat: 43.5948 Lon: -116.3947

Current Scores (2007)	National Scores	State Scores	County Scores
CAP Index	47	97	95
Homicide	56	106	108
Rape	78	151	165
Robbery	42	89	84
Aggravated Assault	55	79	98
Crimes Against Persons	52	84	97
Burglary	70	105	117
Larceny	65	78	84
Motor Vehicle Theft	106	147	135
Crimes Against Property	71	90	96

Scores indicate the risk of crime at a site compared to the average of 100. (i.e. A score of 400 means that the risk is 4 times the average and a score of 50 means the risk is half the average.

Past Scores (2000)	National Scores	State Scores	County Scores
CAP Index	38	87	85
Homicide	48	99	105
Rape	82	133	148
Robbery	35	82	77
Aggravated Assault	43	68	90
Crimes Against Persons	40	72	88
Burglary	55	89	105
Larceny	54	68	74
Motor Vehicle Theft	88	135	128
Crimes Against Property	58	79	85

Future Scores (2012)	National Scores	State Scores	County Scores
CAP Index	51	100	99
Homicide	57	104	105
Rape	83	154	168
Robbery	47	94	91
Aggravated Assault	61	84	101
Crimes Against Persons	58	87	98
Burglary	78	109	120
Larceny	70	81	89
Motor Vehicle Theft	116	151	141
Crimes Against Property	78	93	100

6.3 Terrorism and Extremism

The threat from terrorism is real, it is immediate, and it is evolving. State sponsored terrorism appears to have declined over the past five years, but transnational groups—with decentralized leadership that makes them harder to identify and disrupt—are emerging. Trends show that there are fewer centrally controlled operations, and more acts initiated and executed at lower levels. Terrorists are also becoming more tactically adept and technically sophisticated in order to defeat counter-terrorism measures. For example, as there have been increased security around government and military facilities, terrorists are seeking out "softer" targets that provide opportunities for mass casualties. Some groups are acquiring rudimentary cyber-attack tools. Terrorist groups are actively searching the Internet to acquire information and capabilities for chemical, biological, radiological, and even nuclear attacks.

Potential terrorists do not ordinarily engage in overt criminal activity and are therefore difficult to recognize and intercept. Terrorist organizations are increasingly sophisticated, with educated members linked through technology allowing them to operate from small cells worldwide. Authorities have been reasonably successful in preventing extremism throughout North America; however, the activities of some groups continue to pose a substantial threat.

The threat can be divided roughly into three categories: religious extremism, state-sponsored terrorism, and domestic extremism (including some anti-abortion, animal rights, anti-globalization and environmental groups, and white supremacists).

The number and high profile of international and domestic terrorist attacks during the last decade underscore the determination and persistence of terrorist organizations. Extremist organizations have proven to be relentless, patient, opportunistic, and flexible, learning from experience and modifying tactics and targets to exploit perceived vulnerabilities and avoid observed strengths. Current analysis of terrorist goals and motivations points to domestic and international critical infrastructure and key resources as potential targets for terrorist attacks. As security measures around more predictable targets increase, terrorists are likely to shift their focus to less protected targets.

6.4 Organized Crime

Organized crime has been defined as an ongoing activity, involving a continuing criminal conspiracy having a structure greater than any single member with the potential for corruption and/or violence to facilitate a criminal purpose. Historically motivated by greed and concentrating on profit, criminal organizations have begun to shift focus toward gaining social, political, and economic influence through corruption, intimidation, extortion, and blackmail.

Organized crime groups continue to pose a primary threat to public safety and security in the developed world. They are increasingly fluid, technologically sophisticated, and operate on a transnational level. Organized crime has made money laundering the second largest global industry with the circulation of "dirty" money estimated at $3 trillion worldwide.

Like an amateur, the 'organized' criminals will examine an intended target for vulnerabilities through which to channel their attack. The vulnerabilities may not be apparent to the owner/operator and likely exist within the design elements of a facility, the organizational hierarchy, or an internal business process or system. Identifying vulnerabilities in each of these aspects is an ongoing challenge. To counter this threat, IROC management should initiate a program of annual security threat-risk assessments designed to identify and catalogue vulnerabilities and implement strategies to protect the facility, its assets, and workers. Given the availability of modern sophisticated security systems, an adversary *should* require an uncommon level of technical expertise and determination to be successful.

6.5 Criminal Networks

A disturbing trend is the networking of terrorist, extremist, and transnational organized crime groups. When expedient and mutually beneficial, they have shared strategic resources and logistical support to affect their purposes in locations around the world. In a recent analysis of global trends, the U.S. National Intelligence Council included a short section on criminal organizations and networks. It noted that criminal organizations and networks based in North America, Western Europe, China, Colombia, Israel, Japan, Mexico, Nigeria, and Russia are expanding the scale and scope of their activities by forming loose alliances with one another, with smaller criminal entrepreneurs, and with insurgent movements for specific operations. They are corrupting the leaders of unstable, economically fragile, or failing states, insinuating themselves into troubled banks and businesses, and cooperating with insurgent political movements to assert themselves over substantial geographic areas. In other words, there is a growing recognition that like terrorist groups, organized crime is shifting toward fluid network structures from their formal hierarchies.

6.6 Opportunity Crime

The three necessary ingredients of a crime are motive, means, and opportunity. Of these three, only one—'opportunity'—is within the asset owner's sphere of influence. Reducing the opportunity for crime to occur has the effect of increasing the criminal's risk of detection and apprehension, thereby improving overall deterrence. Amateur (opportunistic) criminals take advantage of low-risk opportunities to perpetrate the majority of their crimes, (crimes of opportunity). Amateurs are not to be construed as unskilled. While they may be disorganized, they are very clever in the use the skills and abilities they have developed through experience; picking 'soft' targets and trusting that their incursions will not be detected until well after their departure.

6.7 Insider Crime

Human nature being what it is, incidents of serious employee theft or fraud occur at some point in every organization. Similar to other crises and problems, internal theft or fraud is as unexpected as it is unwelcome. Investigation and follow-up actions are often poorly handled or not reported, compounding the harm suffered by the organization. Greed, personal situational pressures, addictions, mental illness, and questionable loyalty are all contributing factors. The Association of Certified Fraud Examiners estimated that in 2002 U.S. companies lost six percent of gross revenue to occupational fraud and abuse—the equivalent of $600 billion or roughly $4,500 per American employee.

To understand why the employee potentially represents such a significant threat to the organization, one should first have an appreciation for the motivating causes of personal behavior: personal situational pressures, convenient opportunity, and lack of personal integrity. Personal situational pressures include, but are not limited to, financial instability, high debt, addictions, mental illness, lifestyle choices, and peer group expectations. Convenient opportunities refer to opportunities that are created either by the person or allowed by the organization through a lack of internal controls. Personal integrity is crudely defined as a measure of a person's honesty. While this factor appears to be a straightforward determination of whether the person is honest or dishonest, research of moral development indicates that the issue is more complex. These individuals would normally be expected to act honestly at all times, unless the situational pressures or opportunities to be dishonest were extremely strong. Individuals with low personal integrity may or may not behave honestly, depending on the situation. There may be certain situations in which they consistently behave honestly, but their honesty does not generalize to other situations and is not internalized as a personal value. Their behavior is influenced more by the situation: the opportunity to be dishonest, the probable gain, the likelihood of getting caught, the severity of the punishment, and the perceived need to be met. Most individuals are between these two extremes. A sobering result from studies in some sectors reveals insiders perpetrate approximately 70 percent of all losses.

A discussion about internal threats should not be confined to employees, but rather, should extend to all who are working for, with, or on behalf of the organization regardless of whether or not they are located on the premises. This includes contractors who have regular, unrestricted, and unsupervised access to the building and communications assets. Internal threats also include unauthorized access to or disclosure of sensitive information in the form of document records or electronic data. The Computer Security Institute conducts annual surveys of the Fortune companies and consistently reports that insiders are responsible for the majority of corporate information and data losses.

Losses from stolen or diverted assets are only part of the overall consequences of undetected employee crime. Organizations can become complacent to ongoing losses and even build them into their financial expectations over time. Internal losses are often hidden in the negative variance and not discovered because they are below the allowable threshold and hence not usually investigated.

6.8 Criminal Attack Vectors

The term attack vector represents the various methods an adversary might use to attack or disrupt IROC facilities. Security can be compromised in several ways:

- Fire-alarm Pull – in order to clear the building of anyone who might interfere with an adversary, he/she simply has to pull the fire alarm. In the ensuing confusion, the intruder enters and exits the building before the fire department and facility manager determine that there is no fire.
- Sneak and Peek – an adversary waits until an unsuspecting worker departs the building. Door hardware often takes time to re-latch allowing the intruder an opportunity to sneak behind the unsuspecting worker through the unlatched door.
- Impersonation – an adversary posing as a maintenance contractor, courier, or office or service worker 'tailgates' behind a group of employees during normal business hours. By dressing and behaving appropriately the adversary is able to blend in and roam throughout the building.
- Social Engineering – an adversary initiates and develops a relationship with an employee with the intent of exploiting the organization's assets. The coerced behavior can include theft, fraud, forgery, sabotage, or a range of other criminal activities. Criminal organizations have perfected the art of social engineering in order to gain insight into and penetrate police and other government agencies.
- Disgruntled Employee – this person has a grudge with the employer and is open to an opportunity to settle the score through the misappropriation of assets or the unauthorized disclosure of sensitive information.
- Disgruntled Ex-employee – this person no longer works at the facility but possesses enough building, property, or computer knowledge to seriously disrupt operations.
- Curiosity Exploit – this occurs when an individual with no specific motive discovers a vulnerability, which permits unauthorized access to the facilities assets. Computer hackers or crackers exploit weaknesses in software and network security to determine how far they can penetrate a network or database without being detected.
- Covert Entry – the adversary uses special skills and tools to defeat security technologies to gain undetected access to specific assets within the building.
- Brute Force Attack – direct force to gain entry without regard for detection or apprehension.
- The Bat – an individual positions him/herself in a discreet location within the building and wait until the end of the workday, and then emerges to execute the attack from a position inside the security perimeter.

Table 4 illustrates the various methods and consequences of an attack on mission critical assets.

Table 4 – Methods and Consequences of Attack

Threat, Risk, or Hazard	Method	Consequence
Unauthorized access to the facility	▪ Perimeter doors ▪ Elevators ▪ Stairwells ▪ Interior office spaces ▪ Eavesdropping ▪ Social engineering	▪ Political embarrassment ▪ Loss of public and worker confidence ▪ Asset replacement/repair costs ▪ Liability
Unauthorized disclosure of sensitive information	▪ Steal, forge, or falsify print or electronic records ▪ Obtain personal identification documents (e.g., purses and wallets) ▪ Photocopy strategic plans, procedures, and records ▪ Compromise sensitive briefing notes etc.	▪ Political embarrassment ▪ Unauthorized alteration of records ▪ Privacy violation ▪ Identity theft ▪ Compromise sensitive negotiations or strategies ▪ Liability
Unauthorized access to key personnel	▪ Parkades and parking lots ▪ Change or locker rooms ▪ Cafeterias ▪ Public reception lobby	▪ Personal injury
Unauthorized access to critical communications assets	▪ Computer software ▪ Telephone monitoring ▪ IT Server exploits ▪ Technical surveillance	▪ Damage to or loss of critical infrastructure ▪ Disclosure of sensitive information

6.9 Wild Fire

Fire is a greater and more probable threat than crime. The main cause of wildfires during the spring months is human activity, and therefore preventable. During forest fire season, weather is the controlling factor in the severity and frequency of fires. Lightning is also a major cause of wildfire. The wildland-urban interface exists wherever homes and businesses are built among trees and other combustible vegetation. The wildland-interface fire problem stems from two different sources of fire and their impact on the community. Fires can move from forest, bush, or grassland areas into the community or from the community into the adjacent wild-lands.

On September 26, 2000, the National Interagency Fire Center reported that there had been 1,541 fires in the State of Idaho with 1,235,150 acres burned. A weather pattern called “La Nina” had affected weather across the United States for the previous two years resulting in drought conditions, hot temperatures, low relative humidity, little or no precipitation, and frequent winds.

A review of the data available on Wildlife interface fires indicates that this is not a concern at any of the locations projected for IROC. There is no evidence available that would make wildfire a critical security concern. Note that this speaks only to wildfires, not to fires caused by other means – including accident, spill, or arson.

6.10 Natural Disaster

Flooding, severe weather, earthquakes, forest fires, and health epidemics all fit within the natural disaster definition. The primary effect of natural disasters on critical infrastructure is the disruption of communications, energy distribution, and transportation causing reduced levels of public safety and security resources. Potential climate change during the 21st Century could result in extreme weather events applying significant pressure to emergency response agencies. The frequency of natural disaster events and costs associated with responding to them are both expected to continue to trend upward.

6.11 Traffic

Location is a critical part of the security of a facility. Considerations include neighborhood, adjacent enterprises, quantity and type of traffic, crime rates and projections. The crime rates were dealt with in Section 6.1 and 6.2.

In general terms, the more traffic at a location, the greater danger there will be during an event that would negatively impact the site as a result of that traffic. These events can include hazardous goods spills, major accidents, or the inability of responders to get to the facility during an emergency.

Ada County Highway Department (ACHD) traffic detection volume counts for the arterials near the location options were reviewed. The I-84/Meridian site was the single busiest spot of almost 200 considered, with 56,433 vehicles. The second busiest spot was Eagle Road north of Franklin Road—another candidate location. The Watertower Lane counter, close to the ISP campus, counted 358 cars indicating that this location has the lowest traffic volumes directly adjacent to the location option.

Another concern is that the existing on-ramp to I-84 is at a higher elevation than the IROC facility would be located. This raises several risks:

- Greater surveillance opportunities for a potential attacker;
- Greater access for entry or targeting by projectiles;
- Greater potential impact by a vehicle due to the increased force downhill and from adjacent freeway speeds; and
- The potential for an incident on the ramp or adjacent freeway to spill onto the property, endangering those inside.

The Boise metropolitan area grew in population almost 70 percent from 1990-2005 (206,000 to 345,000). A continuing trend like that would mean 600,000 by 2015, and commensurate traffic issues/risks. If high traffic volumes are presently an issue in some locations, they will be significantly worse when the population doubles again. A more detailed traffic volumes projection is provided in the IROC Location Analysis Report. The resulting analysis based on traffic volume projections from that report conclude:

- Traffic volume projections surrounding the Franklin/Eagle Road location do not support that option as a recommended location for IROC as traffic congestion will likely become more of a problem at that location;
- Traffic volumes in proximity to the ISP campus are projected to double by 2020 indicating consistency in the growth trends of the metropolitan area; and
- Roadway alignment changes along Meridian Road north of I-84 may substantially change the traffic volume projections indicating no comparable judgments can be made on this site regarding traffic volumes.

6.12 Sabotage

Sabotage can result from personal, political, or criminal motivations and is occasionally used to smokescreen other criminal behavior. The term sabotage means the deliberate destruction of property, interference with the production or delivery of goods or services or the undermining of a plan. More often than not, sabotage is perpetrated by an insider—a disgruntled worker who is motivated to seek revenge or one who has been coerced by an outside influence to disrupt the organization. An act of sabotage may involve any one or combination of activities and behaviors described in this report and can be very difficult to predict. Employee security education and situational awareness is the most effective deterrent to sabotage.

6.13 Cyber Crime

The cyber battlefield is real. It is a place where computers are used instead of guns, data packets instead of bullets, and firewalls are used instead of barbed wire. The integrity, reliability, and availability of computer networks and information systems are critical, not only in terms of their ability to perform the necessary functions, but also in terms of their ability to safeguard information without fear of technical intrusion or contamination. All IT network and data systems should be treated as mission critical assets.

Because of advances in technology, critical infrastructure has progressively converged and become interdependent. Those same advances have also resulted in a high and growing level of automation in the operation of communications infrastructure.

The risks common to critical IT resources are many, varied, and often complex: fraud, theft and denial of service, internal mischief, snooping, hacking, spoofing, web server and web browser attacks, virus attacks, mail bombs, impersonation, processor abuse, network intrusion, and corporate/industrial espionage. An adolescent equipped with a computer and a modem connected to a telephone line can, if he/she so desires, become the perpetrator of an attack on an information network. This malicious activity is referred to as Information Operations (IO). Individuals wishing to launch an IO attack could easily find many of its techniques on hacker sites posted on the Web. The resources necessary to conduct an IO attack are now commonplace and it is becoming increasingly possible for even computer amateurs to cause serious harm to computer-dependent systems anywhere in the world. The threat to critical IT networks and information system infrastructure is elevated because of the sensitivity of the data that will be used at the IROC facility. Cyber-threats represent a very real danger to Government and more particularly, to law enforcement and intelligence operations.

6.14 Workplace Violence

Society has evolved to a hectic pace resulting in unwanted stress and personal hardship. This stress often manifests itself in violence and irrational behavior in the workplace. Incidents of violence in the workplace are becoming widespread, organizations should be more vigilant in anticipating and protecting against such incidents.

Workplace violence occurs when a person is abused, threatened, intimidated, or assaulted in his or her place of employment. Workplace violence is not confined to the workplace. It can occur anywhere where a worker might be representing his/her employer. The risks can be influenced by several factors including family or situational pressures, geographic location, time of day, season, and personal health issues. Some occupational groups tend to be at greater risk that others, notably health care and social service agency workers. The result is a toxic work environment with degraded operating performance and potential liability for the employer.

6.15 Catastrophic Events Involving Weapons of Mass Destruction

Terrorist groups are actively searching the Internet to acquire information and capabilities for chemical, biological, radiological, and even nuclear attacks.

A *chemical weapon* is any weapon that uses a manufactured chemical to kill people. What is known as modern chemical warfare began during World War I. The first chemical agent to be used was chlorine gas, about one hundred sixty tons of it, which was released into the wind by the Germans against the Allies. The chlorine floated in huge clouds until it reached the Allied lines causing men to die from the effects of the gas (suffocation). Today, chlorine can be easily acquired in amounts ranging from liters to tons. It is often stored in large quantities at commercial and industrial facilities, often without the appropriate security measures.

Biological weapons use a bacteria or virus, or in some cases toxins that come directly from bacteria to kill people. Biological agents reportedly have been employed to a limited extent during recent military conflicts; however, their use actually dates from antiquity. Intrinsic features of biological agents that influence their potential for use as weapons include: infectivity; virulence; toxicity; incubation period; transmissibility; lethality; and stability. Unique to many of these agents, and distinctive from their chemical counterparts, is the ability to multiply in the body over time and actually increase their effect. The U.S. Centers for Disease Control (CDC) identifies over eighty hazardous chemicals and in excess of 45 biological agents available and releasable for the sole purpose of attacking public health. Many of the substances are found in nature.

Anthrax

Anthrax is an acute infectious disease caused by the spore-forming bacterium Bacillus anthracis and most commonly occurs in wild and domestic animals (cattle, sheep, goats, camels, antelopes, and other herbivores). Although the inhaled form of anthrax is often cited as a potential biological weapon, there are limitations to its use. The bacteria are found in nature, but it is difficult to find strains that will cause serious disease. And once such a strain is found, it is dangerous to handle. Subsequent to the September 11 attacks in New York and Washington, American law enforcement and health officials discovered that Bacillus anthracis spores had been intentionally distributed through the postal system, causing 22 people to be infected with anthrax, leading to the deaths of five of them. Despite the panic that ensued, sending the bacteria in letters does not make an effective biological weapon. Spores of anthrax tend to clump together and fall

to the ground, so they are not easily inhaled. When sent through the mail, the spores are often mixed with light powder that can be inhaled, but sometimes the spores are simply spread on the paper. Even after it is delivered, the bacteria's behavior is somewhat unpredictable. It normally has an incubation period of up to seven days, but could take up to 60 days to develop. And unlike other potential biological weapons, such as smallpox or plague, anthrax cannot be transmitted from person to person, so it will not spread through a population after it has been released.

Smallpox

The threat level of a smallpox outbreak is currently considered low. The virus should only be located in two places in the world: the CDC in Atlanta, Georgia, and the State Research Center of Virology and Biotechnology in Novosibirsk, Russia; however, it is not known if terrorists or other states have obtained the virus. It is only known that smallpox stocks do exist in the world and that terrorist organizations may view the virus to be an effective weapon of mass destruction. There is currently much speculation as to the degree to which terrorist organization and nation-states are actively seeking out chemical and biological weapons. There are a number of ways to spread a chemical or biological agent so that it would infect a large number of people: through the air, municipal water supply, food supply, mail, animals, birds and insects, or through direct human contact.

The most-feared scenario is through the air. The techniques most commonly discussed include:

- An explosion spreading the chemical or biological agent over a wide area;
- An aircraft spraying the agent over a city;
- A vehicle spraying a fine mist along city streets; and
- Aerosol canisters are released inside a building.

The effective dissemination of agents is widely considered to be more difficult than their manufacture. Agents could be delivered to their targets in a myriad of ways, but the most likely are through contamination of food, liquids, vapor or via aerosol within a relatively enclosed area. The popular scenario involving the poisoning of the water supply of a major populations center does not appear to be feasible given the large quantities of agent that would be required and the various filtering or purification measures already in place. On the other hand, the water supply for a discrete installation could be vulnerable, as would be the air conditioning or heating systems of even quite large public buildings.

Radiological Weapons

Radiological weapons are generally felt to be suitable largely for terror, political, and area denial purposes, rather than mass killings. Unlike nuclear weapons, they spread radioactive material contaminating personnel, equipment, facilities, and terrain. The radioactive material acts as a toxic chemical to which exposure eventually proves harmful or fatal. Radiation is energy that comes from a source and travels through some material or through space. Light, heat, and sound are types of radiation. Atom-derived radiation is called iodizing radiation because it can produce charged particles (ions) in matter.

A combination fertilizer truck bomb, if used together with radioactive material, for example, could not only have destroyed one of the New York World Trade Center's towers but might have rendered a considerable chunk of prime real estate in one of the world's financial nerve centers indefinitely unusable because of radioactive contamination. The disruption to commerce that could be caused, the attendant publicity, and the enhanced coercive power of terrorists armed

with such "dirty" bombs (which, for the reasons cited above, are arguably more likely threats than terrorist use of an actual nuclear device), is alarming.

Nuclear Weapons

Nuclear weapons are the most destructive technology ever developed. Nuclear explosions produce both immediate and delayed destructive effects. Immediate effects, including blast and thermal radiation are produced and cause significant destruction within seconds of a nuclear detonation. The delayed effects (e.g., radioactive fallout) inflict damage over an extended period ranging from hours to centuries, and can cause adverse effects in locations very distant from the site of the detonation. While they have yet to make their appearance as the weapon of choice for anyone but a few nation states, it has long been feared that nuclear weapons would one day find their way into the hands of criminal, terrorist, or extremist organizations.

Explosives

The frequency of the use of explosives by criminals and terrorists has been growing steadily since the early 1970's when readily available commercial and industrial chemicals were first combined to formulate simple but effective 'homemade' bombs. Known as an improvised explosive device (IED), the homemade bomb is still the weapon of choice for many who do not have access to more sophisticated military munitions. An IED is a device that is designed to cause death, injury, or damage by using explosives alone or in combination with toxic chemicals, biological toxins, or radiological material. IEDs can be produced in varying sizes, functioning methods, containers, and delivery methods. IEDs can utilize commercial or military explosives, homemade explosives, or military weapons and weapons components. Designed to defeat a specific target or type of target, they generally become more difficult to detect and protect against as they become more sophisticated. IEDs fall into one of three types: packaged, vehicle, and suicidal.

Packaged IEDs are typically placed near or delivered to their intended target. Sometimes they are thrown and occasionally they have been hidden inside construction elements of buildings during construction.

Vehicle IEDs (car bombs) are devices that use a vehicle as the explosive's package conveyance. Car bombs have appeared in all shapes and sizes, from small sedans to large cargo trucks. In some parts of the world, there have been instances where explosives were found inside generators, animal carts, and even emergency vehicles. Obviously, larger vehicles can accommodate larger amounts of explosives, ranging anywhere from 100 pounds to well over 1,000 pounds.

A suicide bomber is a singularly difficult threat to counteract. The aim of the suicide bomber is not to commit suicide but to kill or injure as many other people as possible. A "person-borne" bomb usually combines a high explosive with fragmentation and uses a detonator switch or button the person activates. The explosives and the fragmentation particles are contained in a vest or in clothing that have been modified to carry the materials. Deadly force is normally the only effective response option to a suicide bomber.

When an explosive device is detonated near a structure it creates a pressure wave of energy that should be absorbed by and transferred through the building front and interior structural components. Blast pressures at the explosion site are very high but decrease rapidly with distance. The two parameters that most directly influence the blast environment that the structure will be subjected to are the bomb's charge weight and the standoff distance. The property owner has no

influence over the first of these parameters. The design strategy should be to maintain as much standoff distance as possible and harden the facility for the resulting blast pressures. Barriers on the perimeter of the resulting standoff zone maintain the required standoff distance. Vehicle barriers should be capable of stopping a moving vehicle at the perimeter of the standoff zone.

6.16 Findings

- The 2005 group "A" criminal offense overview for the State declined by 4.7 percent over 2004 and declined by 0.5 percent in Ada County during 2005. The group "A" crime rate per 100,000 population in Ada County was 7,230, whereas in Meridian it was 6,132 (14 percent below the County average but still a 7.5 percent increase year over year for that community).
- Candidate locations 1, 2, 3, and 5 were near-equal in their respective National CAP Index Scores of 51 and 52. Candidate location 4 had the lowest National CAP Index Score of 47.
- Current analysis of terrorist goals and motivations points to domestic and international critical infrastructure and key resources as potential targets for terrorist attacks. A disturbing trend is the networking of terrorist, extremist, and transnational organized crime groups.
- Terrorist and extremist groups are actively searching the Internet to acquire information and capabilities for chemical, biological, radiological, and even nuclear attacks.
- Organized crime groups continue to pose a primary threat to public safety and security. There is a growing recognition that like terrorist groups, organized crime is shifting toward fluid network structures from their formal hierarchies.
- Amateur, opportunistic criminals (both insiders and outsiders) continue to take advantage of low-risk opportunities to perpetrate the majority of their crimes utilizing over a dozen potential attack vectors.
- Fire is a greater and more probable threat than crime. Modern communications and data centers undergo enormous pressure during crisis events. Fires inside these types of facilities are caused by electrical faults in raceways, cable trays, beneath raised floors, and inside other concealed areas.
- The frequency of natural disaster events and costs associated with responding to them are both expected to continue to trend upward.
- Cyber-threats represent a very real danger to Government and more particularly, to law enforcement and intelligence operations.
- Incidents of violence in the workplace are becoming widespread, and in the interests of public safety, organizations should be more vigilant in anticipating and protecting against such incidents.

Recommendation

Given the value, sensitivity and criticality of IROC it should be located at the site adjacent to the ISP campus or the site at the intersection of I-84 and Meridian Road. These present the most secure starting point for the site, with easy access for police and emergency response. Although ISP may present more of a target for determined attackers than the other participating agencies, an ISP campus location will also deter less motivated attackers. The development business continuity and emergency response plans is critical to the long-term security of IROC.

7. RISK EQUATION

Various agencies and research think tanks have developed a methodology to quantify risk to a certain degree, via the use of formulas. FHWA has utilized such a methodology for such as Traffic Management Centers of Emergency Operations Centers. Although the threat risk assessment for IROC is intended to be qualitative, this section will discuss the application of the quantitative method to this project.

The actual equation is RR = TA x T x C x (1-LD) x (1-LS) where:

RR = Relative Risk

TA= Target Attractiveness

T = Threat

C = Consequences

LD = Deterrence

LS = Security system Effectiveness

While this methodology can provide insight, it is important to understand that assigning raw numbers to the evaluation of risk can often cloud the issue and requires a certain level of guesswork and assumptions about both the attacker and the security systems. Also, the methodology is typically undertaken at a facility where multiple assets are ranked and protected according to their value. In this case, the facility will be studied as a whole, as a single asset with a single security system. Ranking and protection of individual assets is included elsewhere in this document. With that caveat, this section will walk through a Relative Risk equation for this site.

7.1 Target Attractiveness

The following table is taken from the U.S. Department of Transportation FHWA Guide to Physical Security Risk Management for Traffic Management Centers. Interviews with the stakeholders for IROC helped to develop scoring for the table, which helps to determine the level of security required at the facility. This methodology was used in this case as a cross-check to validate the findings already developed through the interview process.

Factor	Rating	Score	Example Criteria
Knowledge of Existence	*How well known is the facility or asset?*		
	Very High	5	Outside the State
	High	4	Statewide
	Moderate	3	Regional
	Low	2	Local
	Very Low	1	Secret or unknown facility or asset

Factor	Rating	Score	Example Criteria
Availability of Information	*How available to the adversary is information about the facility, asset, security measures, etc.?*		
	Very High	5	Widely available to the public or in plain view of persons off the controlled property
	High	4	Information is available to the public
	Moderate	3	Information is available only upon request
	Low	2	Information is closely held or proprietary
	Very Low	1	Information is classified and protected as such
Symbolic Importance	*To what extent does the facility represent the U.S. government, capitalism, etc.?*		
	Very High	5	Prominent U.S. government building
	High	4	Tenants include only U.S. government agencies or some high-risk agencies (law enforcement)
	Moderate	3	Tenants include some U.S. government agencies
	Low	2	State or local government building
	Very Low	1	Not a government facility
Publicity Generated	*What is the extent of publicity that would be generated by an attack or attempt?*		
	Very High	5	Worldwide
	High	4	Nationwide
	Moderate	3	Statewide
	Low	2	Local
	Very Low	1	Site or organization only
Ideology	*How well does the target suit the ideology of any known ideological adversary?*		
	Very High	5	Suits multiple known ideologies well
	High	4	Suits multiple known ideologies
	Moderate	3	Suits a single known ideology well
	Low	2	Suits a single known ideology
	Very Low	1	No ideology other than anti-U.S. sentiment
Mass Casualty Potential	*What is the potential for mass casualties of an attack at the facility?*		
	Very High	5	More than 100 persons on-site or in close proximity to target
	High	4	51-100 persons on-site or in close proximity to target
	Moderate	3	26-50 persons on-site or in close proximity to target
	Low	2	11-25 persons on-site or in close proximity to target
	Very Low	1	0-10 persons on-site or in close proximity to target

Factor	Rating	Score	Example Criteria
Perceived Criticality	*How critical to operations and government services is the asset (perceived or in actuality)?*		
	Very High	5	Critical to continuity of government operations
	High	4	Critical to public safety
	Moderate	3	Critical to essential government services
	Low	2	Moderately critical services
	Very Low	1	Non-critical
Economic Disruption	*How widespread would the economic impact of loss of the target be?*		
	Very High	5	Worldwide or substantial nationwide
	High	4	Nationwide or substantial statewide
	Moderate	3	Statewide or substantial regional
	Low	2	Regional or substantial local or site/organization
	Very Low	1	Local or site/organization only
Public Confidence	*What is the extent of the impact of an attack or attempt on public confidence?*		
	Very High	5	Worldwide or lengthy nationwide
	High	4	Nationwide or lengthy statewide
	Moderate	3	Statewide or lengthy regional
	Low	2	Regional or lengthy local
	Very Low	1	Local or very limited impact
Level of Effort	*What is the level of effort required to prepare and carry out an attack against the target?*		
	Very High	5	All 3 – Extensive stockpiling of materiel, multiple accomplices, extensive reconnaissance
	High	4	2 out of 3 – Extensive stockpiling of materiel, multiple accomplices, extensive reconnaissance
	Moderate	3	1 out of 3 – Extensive stockpiling of materiel, multiple accomplices, extensive reconnaissance
	Low	2	Some materiel, few or no accomplices, limited to no reconnaissance and planning
	Very Low	1	Asset subject to attack with hand tools by a lone adversary with little to no prior planning

Interviews have indicated that the overall impression of Target Attractiveness is a raw score of 34 (4-3-4-3-4-3-4-2-3-3). This raw score indicates that IROC would be an above average target *for attackers who wish to operate in Idaho.*

This finding is consistent with the information generated by the interviews, and helps to identify the level of security that will eventually be required at IROC.

7.2 Consequence Evaluation

If terrorists, thieves, disgruntled employees, or others attack a facility, there are a number of ways that consequences can occur. Several of the factors have been selected that are consistent with the TMC Risk Management Guide for the purposes of this study. The factors selected were:

- Casualties – Dead/Injured as a result of a particular event;
- Mission Downtime – How long IROC would be out of commission as a result of the event;
- Economic Impact – Direct economic impact stemming from an event; and
- Downstream Effects – Impact on the transportation system.

An interview process had personnel involved in this project at various levels evaluate these consequences based on five different scenarios of various potential consequence. These scenarios included:

- *Scenario 1*: Terrorist or other well-prepared attacker uses vehicle bomb in the parking lot of the facility.
- *Scenario 2:* Attacker with malevolent intent breaks into the facility and does serious damage to the control room, server room, or other critical areas. No weapons are available.
- *Scenario 3:* Break and Enter to the site, destruction of some property, theft of computers. No weapons. This is an after hours attack.
- *Scenario 4:* Destruction of external communications infrastructure. Explosives are used.
- *Scenario 5:* Angry client or ex-employee attacks via the main entry point. Intent is to injure persons, damage property. Small arms may be available to the attacker.

The results of the interviews on this subject were consistent with expectations. The five scenarios scored as:

- Scenario 1: Consequence Factor of 4 (of a possible 5). This indicates very high negative impact if this scenario occurred.
- Scenario 2: Consequence Factor of 3 (of a possible 5). This indicates high negative impact if this scenario occurred.
- Scenario 3: Consequence Factor of 2 (of a possible 5). This indicates medium negative impact if this scenario occurred.
- Scenario 4: Consequence Factor of 3 (of a possible 5). This indicates high negative impact if this scenario occurred.
- Scenario 5: Consequence Factor of 3 (of a possible 5). This indicates high negative impact if this scenario occurred.

All scenarios would negatively impact the facility and its ability to achieve its mission. None of the scenarios graded as low consequences, therefore all must be protected.

In particular, some consequences would move beyond solely the traffic management aspects of IROC. As an example, in the event that State Emergency Medical Services (EMS) operations went down while housed at the IROC facility, State EMS would require activation of back-up facilities located at the Department of Health and Welfare Central Office in Boise. During the course of moving to the back up facility, State EMS would notify Idaho Transportation Department (ITD) Headquarters that all dispatching services would revert back to the District level, which would not happen instantaneously. State EMS would also notify numerous county

law enforcement agencies as well as several state agencies of the move and that until the back up facility was open and phone lines have been transferred, State EMS will not be able to dispatch emergency medical service units or receive reports of any other situation that may be taking place. Standing up the back up facility could take up to an hour depending on speed of transferring phone lines and getting staff to the center. The time lag that would occur in the transfer to back up, or alternatively the possibility of the back up facility not being available, requires that IROC be as self sufficient as possible. If the Department of Health and Welfare central office was also damaged or unavailable for some reason, all services performed by State EMS would come to a halt with the exception of ITD taking back dispatch control at the district levels. The way to achieve this is indicated in the various recommendations throughout this report; however, the essence of it is that this facility would become critical to State EMS, and must be secured and provided with reliable backup systems to prevent loss of stakeholder capability.

7.3 Deterrence

The final parts of the risk equation are deterrence and security system effectiveness. The methodology uses percentages to rate deterrence and effectiveness, with Very Low equivalent to 0.1, Low equivalent to 0.3, Medium equivalent to 0.5, High equivalent to 0.7, and Very High equivalent to 0.9. Note that these are necessarily subjective ratings based on the experience of the personnel performing the task.

For the purposes of this document, both deterrence and systems effectiveness is rated as “Very Low”, or 0.1, for baseline evaluation. The second calculation will assume incorporation of the Recommendation in building the facility, and will rank both criteria as “Very High”, or 0.9.

For our purposes it is appropriate to score deterrence and system effectiveness evenly, as the recommendations are designed to raise the level of both of these elements of security.

7.4 Threat

The threat component of the equation is one of the most difficult to assess. The bulk of this report is the discussion of the various threats, and the incidence of occurrence; however, there can never be absolute certainty what the real threat is to the facility. Without 100 percent effective intelligence about all potential attackers, which is not possible, there can only be educated estimates of the potential for an occurrence. The methodology therefore utilizes the existing DHS Threat Condition to provide a value for the threat. Threat Condition Yellow is rated a “1”, Orange is a “2”, and Red is a “3”. The present threat condition (as of this writing) is Yellow.

7.5 Calculations of Risk

Given the information above, the Risk Equation is incorporated as follows:

RR = TA x T x C x (1-LD) x (1-LS)

The Base Evaluation (no countermeasures)

	Relative Risk	Target Attractiveness	Threat	Consequences	Deterrence	Effectiveness
Scenario 1	12.9	4	1	4	0.9	0.9
Scenario 2	9.7	4	1	3	0.9	0.9
Scenario 3	6.5	4	1	2	0.9	0.9
Scenario 4	9.7	4	1	3	0.9	0.9
Scenario 5	9.7	4	1	3	0.9	0.9

Using this methodology, the worst possible relative risk score would be 60.75 if the threat condition were Red. With threat condition Yellow, the highest possible Relative Risk score is 20.25. If the formula were re-run assuming very high deterrence, detection, and response, the results would change dramatically.

	Relative Risk	Target Attractiveness	Threat	Consequences	Deterrence	Effectiveness
Scenario 1	1.2	4	1	4	0.1	0.1
Scenario 2	0.1	4	1	3	0.1	0.1
Scenario 3	.08	4	1	2	0.1	0.1
Scenario 4	0.1	4	1	3	0.1	0.1
Scenario 5	0.1	4	1	3	0.1	0.1

It is clear, even given the various assumptions and the subjectivity employed, that the use of strong countermeasures greatly reduces the relative risk to the facility.

It is important to note that in ranking system effectiveness and deterrence with very high scores, it was assumed that most or all of the recommendations in this report would be carried out. These recommendations will speak not only to electronic systems such as access control and closed-circuit television (CCTV) cameras, but just as importantly to procedural security, design standards, and monitoring, maintenance, and auditing of the security program. Leaving any of these aspects by the wayside will certainly reduce the system effectiveness and the deterrence capability below the desired “Very High” has been applied.

8. VULNERABILITIES

Because of the value, sensitivity, and criticality of the assets under protection, this facility should be treated as a high-security venue. Securing the facility begins with establishing a series of outer and inner perimeters that are equipped to deter, detect, delay, and defend against an attack or a criminal act. These perimeters need not always be physical in design and appearance. Choosing an appropriate combination of physical, logical, and electronic security measures will enhance overall facility security and improve the return on investment.

Physical Measures

Physical security consists of physical and psychological barriers, (e.g., walls, doors, glass, floors, ceilings, and signage), locking hardware and security lighting, collectively known as 'the security infrastructure'.

Logical Measures

The term 'logical security' applies to the plans, policies, procedures, and employee security awareness that combine to support the physical security elements intended to protect the assets from harm. Logical security measures are designed and implemented to provide direction and guidance to individual workers regarding the nature and location of the assets under protection, describe their individual roles and responsibilities concerning asset protection and instruct them in how they should interface with the physical security measures deployed in the facility. Without logical security measures, asset protection is left to the discretion of each individual.

Electronic Measures

Electronic security measures include automated access control, intrusion detection, CCTV, and software integration to enable the systems to interact with one another to facilitate event detection, assessment, response, and post-event analysis.

8.1 Characterizing the Security Requirement

Each building is a six-sided structure consisting of base building construction elements, interior partitions, utility inter-connects, entrance and egress points, and electrical/mechanical components.

The facility should be divided into four security zones.

- The public/reception zone is that area to which the general public has unimpeded access during normal business hours. It will be constructed and equipped to prevent unauthorized entry to the remaining portions of the building.
- The administrative zone(s) are those that accommodate administrative assets and activities and may include the common-use areas (i.e., break and restrooms). This zone will be physically partitioned from the other zones.
- The operations zone(s) are those that accommodate assets and activities of an operational nature, (i.e., operator workstations, break, locker, storage) and will be physically partitioned from the other zones.
- The secure zone(s) are those that contain high criticality assets or activities, (i.e., IT network and data server rooms, telecommunications closets, electrical/mechanical/HVAC compartments).

The internal business processes will also be in need of protection, for example mail handling, catering, and services. The graphic below illustrates a layered approach to protecting both assets and processes.

The center represents a mission critical asset. Each sector of the dart board represents an internal business process involving those particular assets. Each concentric ring represents a layer of security uniquely designed to protect both the asset and its associated business processes. Designing the physical, logical, and electronic security measures into both the facility and its internal business processes ensures the organization's security objectives will be met.

Each of the areas or processes noted below present a vulnerability to the effective operation of the facility as a whole. Discussion of the vulnerability occurs, with recommendations to secure the vulnerability in the Recommendations section,.

8.1.1 Public Access

The ITD and ACHD have indicated a need for public and media access to the facility. This increases the potential for unauthorized persons to gain access to secure areas.

8.1.2 Motor Vehicles

One of the most basic tenets of security, especially for a secure facility, is to limit the approaches to the facility, and to control who is allowed on or off the site. While reducing the number of vehicle access routes does much to enhance control and monitoring of vehicles, it has the opposing effect of 'putting all of one's eggs into one basket'. The number of vehicle access points will determine the property's ability to continue operating in spite of external interference. A serious motor vehicle accident (e.g., pedestrian collision) at or near the facility's vehicle access/egress points may temporarily disrupt the flow of traffic to and from the property. Planning for emergency/alternative vehicle access/egress routing should be included in the early planning phases of the project to mitigate this potential threat.

Vehicle checkpoints will no doubt be employed to identify vehicles, occupants, and cargo during periods of heightened security. The architectural landscape design should take into account that each checkpoint should enable thorough inspection and prevent a vehicle from moving into the security perimeter until its entry has been approved. This may entail the presence of a processing area where vehicles can be safely parked while undergoing an inspection and a turnaround large enough to accommodate commercial vehicles denied access.

Vehicle traffic peaks will occur at the beginning and end of each work period. A serpentine vehicle approach route coupled with multi-lane terminal parking lot will serve to 'calm' traffic, facilitate surveillance, and distribute vehicles to assigned parking sectors while minimizing wait times for arriving and departing traffic. The size of the site indicates that probably only one diversionary turn or barrier is necessary.

8.1.3 Parking

Providing secure parking for employee and state vehicles will be a necessity. One area of the facility in which physical and human resource assets are exposed to sources of harm is the parking lot. Parking structures, whether above or below ground, are often perceived as dark, isolated, confined, and confusing places with little apparent security. Parking areas should be designed with clear sight-lines. Individual parking spaces should be perpendicular to driveways. Parking garages should utilize round columns to minimize hiding opportunities and their walls should be painted with a reflective paint. The parking area design should allow continuous observation of:

- Vehicle and pedestrian approach and departure routes;
- Parked vehicles;
- Floor plates (enclosed parking garages); and
- Perimeter security devices (e.g., fences, gates, doors etc.).

Parking lot security is maintained using either passive or active security measures. Passive measures include lighting, fencing, and signage and so on. Active measures include CCTV, duress alarm stations, intercom sets, security patrols etc.

Parking area access controls are intended to decrease criminal opportunity by guiding, controlling, and monitoring movement. The design should be logical and:

- Assist first-time users find their way to their destination;
- Monitor, examine, and if necessary, quarantine a vehicle prior to its entry to the parking area;
- Permit large vehicles to turn around without entering the parking area or disrupting traffic flow;
- Route vehicles to their designated parking areas;
- Prevent unauthorized vehicles from entering the 'secure' parking areas;
- Enable certain parts of the parking area to be temporarily 'locked-down';
- Deter, detect, and report unauthorized vehicle or pedestrian traffic; and
- Enable rapid departure/evacuation.

These measures are consistent with both commercial and government buildings, across the country – they describe methods of applying both safety and security at one of the weakest links in any facility. In particular, measures in a parking lot need to address safety for employees – lighting and controlled access are important to keeping a safe environment here.

8.1.4 Internal Access

There will be a need to have persons on-site from time to time who are not employees. This group would include tours, contractors, vendors, and repair personnel. If they are not effectively controlled they can present a huge risk to the facility. This is not limited to persons who are malevolent in their intent, but with the amount of communications, networking, and computer equipment in the facility it would be relatively easy for a curious person to cause problems if they were not properly escorted.

8.1.5 Local-Area Network/Wide-Area Network

The network infrastructure of the facility will be a prime target for any attacker. It is now generally understood, in this electronic age, that access to an organization's internal networking is an effective way to preventing them from achieving their mission. Networks are also targets of opportunity for hackers. Control of the network is a critical component of the overall security of the facility.

8.1.6 Secure Collocate Facility

The nature of this facility is such that different agencies will be sharing common space for network and computer functions. This can be an issue, as someone could inadvertently or malevolently damage equipment or processes. A secure collocate facility for servers and other computer equipment will be required.

8.1.7 Communications

Communications are the reason for the existence of the IROC facility. Exposing any critical component of the communications infrastructure to risk is not acceptable.

8.1.8 Meeting and Conference Rooms

Meeting and conference rooms are considered a vulnerability when they are to be used with outside personnel. Effective controls at both the physical and logical level are required to ensure these rooms are not a soft target.

8.1.9 Common Spaces

The common spaces would also include lunch rooms, locker and change areas, and any area that is not specific to an agency or purpose. It is not unusual to find that common spaces are a forgotten "back door" into a site. For example, one can often find a lunch room door to a facility open to the outside, propped to accommodate persons entering and exiting to smoke.

8.1.10 Emergency Power and Fuel Storage

Emergency power and fuel storage are a major factor in the Business Continuity planning process. Loss of power, or fuel to back up generators, can render the facility useless as fast as a break in or explosion would. Typically fuel storage will be dictated to some extent by the local building and safety codes. These will indicate whether a fuel storage area can be underground or not. During the design phase of the project the site will be designed such

that fuel storage is secured. Design strategies may include such techniques as applying stand off distances and ballistic walls as necessary for above ground tanks and electronic monitoring of the area near the storage. Another critical consideration to be addressed during detailed design would be fuel delivery procedures. This is addressed as part of the overall need for site specific security policy and procedures.

8.1.11 Communication Antennas

A facility such as IROC will certainly require some outdoor antennae in order to receive and transmit the information that is the purpose of the project. Because these antennae should be outdoor, they are a visible and obvious target for attackers. Redundancy and physical protection are the appropriate security choices

8.1.12 Mail and Courier Traffic

This category would also include service entrances. Again, this is one of the most ignored vulnerabilities in most buildings. How are couriers handled? Are they provided access beyond the main door/gate? Do service personnel enter the building unaccompanied and unwatched? Are they all accounted for at all times? These issues should be addressed in the security program design.

8.1.13 Critical Dependencies

Identifying and protecting IROC's critical internal and external dependencies will involve the development of Emergency Preparedness, Disaster Recovery, and Business Continuity Plans. These plans will integrate with the security policy and procedures to ensure that the facility is protected from a disruption that would render it ineffective.

Internal

Internal dependencies include safety equipment and training for the personnel and adequate supplies to sustain the facility through a protracted disaster event that would otherwise impair the Center's operation.

Redundant power supplies, communications equipment, fuel, food and water are needed to ensure that if and when the external service providers fail, the Center can continue to fulfill its mission for at least 72 hours.

External

The external dependencies include water, sewer, electrical power, gas, and communications infrastructure that are, for the most part, beyond the ability of IROC to control or protect. Ensuring that essential back-up services and supplies are assured through mutual aid and vendor supply agreements becomes essential to the facility's ability to fulfill its mission.

9. RECOMMENDATIONS

The following section is provides recommendations that are relevant to the intended security program at IROC. Recommendations have been developed from several sources. First is the analysis of the data provided previously in this report – the existence of particular threats and hazards. Secondly, the

specific needs of the participating agencies are considered. Next is a consideration of the best practices relevant to both security generally, and these types of facilities in particular. As in any business process, there are always options in how to achieve a particular goal. Best Practices indicate what the ideal situation may be, and provide a measuring post for the upgrades necessary. These security Best Practices are an incorporation from several sources:

- US Military publications related to Physical Security;
- Federal Emergency Management Agency (FEMA) publications;
  - FEMA 426 Reference Manual to Mitigate Potential Terrorist Attack Against Buildings;
  - FEMA 427 Design of Commercial Buildings to Mitigate Terrorist Attack; and
  - FEMA 386-7 Integrating Human Caused Hazards Into Mitigation Planning.
- TMC Risk Management Guide;
- American Society for Industrial Security – Protection of Assets Manual;
- Federal Communications Commission/Public Safety Answering Point Emergency Planning Guidelines;
- CDC, Guidance for Protecting Building Environments from Airborne Chemicals, Biological, or Radiological Attacks; and
- Consultant Experience.

This facility is somewhat unique in the security approach to be taken because there are multiple stakeholders. Typically, each stakeholder has their own specific security requirements, and normally can design and implement a security plan to meet those needs. In this case however, the fact that the most critical areas of the facility will be shared requires that security programming and design be approached from a "highest level necessary" point of view. This will mean that for all shared areas, all stakeholders will have to accept the most stringent level of security required by any of the other stakeholders.

Ultimately, these recommendations will be discussed and implemented as necessary during the eventual design phase of the project.

9.1 Physical Security

9.1.1 Buffer Zones

A buffer is the area outside the secure perimeter of the facility. Depending on the site, IROC may have little or no control of these areas, however, it is from this buffer zone that attacks on the facility will be staged and launched. Accordingly, consideration of the buffer zone should figure into security planning. After the threat assessment identifies threats and vulnerabilities, preventative measures for the buffer zone should reduce the risk by a four-step process:

- Devaluing a target by making it less attractive or too costly to attack;
- Deterring an event from happening (i.e., through warning signs, physical barriers, cameras, and security guards);
- Detecting a person who is planning or committing an attack or the presence of a hazardous device or weapon; and
- Defending against attack by delaying or preventing an aggressor's movement toward the asset or use of weapons and explosives.

The important component is recognizing these core issues and addressing them through various technologies and processes when the geography permits. As an example, the use of signage, CCTV, random guard patrols, and visible lighting are all effective means of addressing buffer zone security, even in difficult environments. Crime Prevention Through Environmental Design (CPTED as described in more detail in a subsequent section) concepts are also extremely effective methods to maintain some control of the buffer zone.

9.1.2 Stand Off Distance

A stand off is the area around a building or site from which a person or structure could withstand explosion beyond a given distance. Design strategy should be to keep intruders as far away as possible. It is not always possible, in particular with existing facilities, to provide appropriate stand off. That does not eliminate the need to consider stand off distances in design.

The stand off distance table below provides appropriate standards for given levels of protection. This table is acquired Department of Defense Unified Buildings Criteria.

	To Controlled Perimeter	**To Stand Off**
Inhabited Building	30 ft (10m)	80 ft (25m)
Critical Building	80 ft (25m)	150 ft (45m)

It is important to note that the stand off distance also encompasses parking areas.

9.1.3 Perimeter Demarcation

All perimeter fences and walls should be a minimum of eight feet in height with three strands barbed wire on chain-link fence, and other anti-climb devices on masonry walls. Where viable, a barrier footing should be included as part of the fencing structure. Other detection and assessment tools should always be used in conjunction with perimeter barriers.

The entire perimeter of each property should be well separated. Signs, hedges, ditches, and fences provide a psychological deterrence to trespass. Perimeter landscapes should deny the intruder a place to hide by keeping grass and shrubs trimmed and trees cleared away from the facility. This is especially important if there is a threat to night shift personnel. More specifically, there should be a clear space of three meters around buildings and on both sides of paths between buildings and parking areas, sidewalks, and public transportation stops. Objects such as paving stones, bricks, and outdoor furniture should be fastened or removed so as to prevent their use for offensive purposes. Landscaping features can also be used to prevent vehicle access to a facility.

A barrier is often used as the first line of defense in protecting a facility and thus is a critical element of perimeter defense. The chain-link fence is the most common of these barriers, owing to its durability and relatively low cost; however, it should be clearly understood that the use of a fence or wall is at best a deterrent to casual intruders and a delay to other intruders. It should in no way be considered an effective security mechanism standing alone. A determined intruder will easily circumvent most fence barriers, chain-link or

otherwise. The use of detection and assessment tools, such as fence alarming and CCTV, enhances the barrier function to provide a useful security countermeasure.

Recommendation

The perimeter barrier will depend on the final location. Chain link fence with barbed wire is probably not viable in more public locations. A development at the Franklin and Eagle location would need to take into account the aesthetics of the residential area nearby. Locating near the highway (I-84) would likely provide more flexibility in terms of types of fencing. The ISP campus already has a certain level of perimeter fencing – development on the tract north of the campus would allow installation of a perimeter fence with some controlled public access.

9.1.4 Gates

Sliding gates should be used, rather than swing gates.

Gates are a critical element of the perimeter, and typically a weak point for entry. They should be made of material matching the strength of the fence and equipped to prevent easy removal. Gates should have a predetermined opening and locking protocol and procedures that promote responsible use. Gates should be monitored during business hours and secured after business hours to prevent access by automobiles and pedestrians. Gates should be secured with high-quality locking devices. Barbed wire topping is only likely to discourage young and inexperienced intruders.

One of the major issues in gating is the strength of the gate when attacked or hit by a vehicle. Swing gates that join in the middle of the road provide minimal protection from this type of attack. The center point where the gates meet is the weakest area, and a vehicle attacking this point can easily breach the gate. The use of a sliding gate eliminates this weak point and establishes the quality of the gate material itself as the major variable in its ability to withstand attack.

Recommendation

There should be at least two entry/egress points to the facility, to provide a secondary route in the event of man made or accidental blocking of one point. The secondary entry point could be used for emergency purposes only. All site entry points are recommended to have controlled, alarmed, rolling metal gates that can be secured as necessary – after hours, or on raising the security level at the site.

9.1.5 Interior Roadways

Roadways inside the facility should be constructed in such a way as to prevent a vehicle from having a long, straight run at any asset, particularly the critical areas. Traffic calming via roadway circles and frequent direction changes is usually recommended. Also, parking areas should be far enough away from major or critical buildings to provide a standoff area for explosives.

Recommendation

The existing communications building on the ISP campus provides a long, straight run up to it for a vehicle. This is not appropriate, even with a gate further down the road presumably

limiting access. Design at the new site should accommodate roads as described above, alternatively the use of bollards or berms should be considered. The architects should take into account parking standoff distances.

9.1.6 Lighting

Adequate light should be provided for deterrence, safety, CCTV, and guard patrols.

Recommendation

Visible light will be necessary in the parking areas. Locating at the ISP campus should allow a significant amount of visible light to be available. Locating at one of the other sites may require less light to accommodate residential needs nearby. In this case, the use of IR lighting would be necessary for exterior surveillance.

9.1.7 Crime Prevention Through Environmental Design

CPTED should be considered when designing or expanding a facility.

CPTED is the derivative of work begun in the 1960's and continued since, by several architects/law enforcement personnel, notably Ray Jeffrey and Oscar Newman. The several books authored on the subject developed general guidelines on the subject. These guidelines are not formal, nor are they issued by any particular government agency. They are, however, understood as effective practice in both the architectural and security fields. Department of Homeland Security has issued a document titled Conducting CPTED Risk Audits for Anti- Terrorist Infrastructure Protection. This document, while not necessarily a formal "Guideline", accurately reflects the critical components of CPTED thinking.

The goal of CPTED is to create and maintain an environment where landscape and interior design leads to a reduction in the occurrence of crime. The three overlapping CPTED design strategies are:

- Exploit natural surveillance;
- Capitalize on natural access controls; and
- Enhance territorial reinforcement.

Exploiting natural surveillance means:

- Design the space to facilitate observation by maximizing visual observe-ability;
- Balance the need for privacy against the need for personal safety by placing vulnerable activities in locations that can be easily monitored;
- Strategically orient work spaces and other activity centers toward the areas of vulnerable activity; and
- Ensure that each phase of the project takes advantage of and enhances natural surveillance opportunities. This is particularly critical with respect to landscaping and lighting.

Capitalizing on natural access control means:

- Decrease criminal opportunity by effectively guiding and monitoring vehicle and pedestrian traffic;

- Provide for "eyes on the street" through the strategic placement of entrances, windows, etc.;
- Route access to the facility through observable areas and prevent access to unobservable areas;
- Provide people with a sense of direction while giving them some natural indication as to where they are and are not permitted, (way finding);
- Provide a limited number of access routes while allowing users some flexibility in movement; and
- Ensure that natural access control opportunities enhance and complement natural surveillance objectives.

Recommendation

Design team needs work with the landscape architect to ensure security is not compromised by aesthetics. Additionally, the CPTED design will incorporate the comments on interior roadways and parking above.

9.1.8 Signage

Signage design should balance two critical needs: (1) to provide information to persons on the grounds, and more importantly to police, fire, or ambulance responders, and (2) to not provide so much information that they can aid an intruder in his/her actions. Signs for public use should only detail areas the public is allowed to access, and not mission-critical or high risk areas where the most damage can be achieved. The design approach to signage on-site should consider three types of signs:

- Building-identifying;
- Wayfinding; and
- Regulatory/warning.

Recommendation

Perimeter warning signs are recommended regardless of the location chosen. This at the very least clearly defines the boundaries of the facility. Wayfinding and identification signs will be necessary to incorporate the expected building into two areas, across the street from one another as applicable.

9.1.9 Building Surfaces

An analysis of building surface requirements for security purposes will take into account the nature and criticality of the assets contained in the facility, the length of time those assets might be left unattended, the consequences of the loss of the assets, and the cost of repair/replacement.

Most building surfaces are at least two layers thick. Exterior surfaces are normally designed to support structural elements and protect the interior from the elements, not from forced attack. It can take as little as 45 seconds to get through an eight-inch mortar filled concrete block wall using a 10-pound sledge. Modern cutting tools can reduce that time even further. An IED can cause heavy damage to or total loss of a facility. IEDs are quickly becoming the penetration method of choice while being the most difficult to defend

against; however, blast damage is only one of several considerations. Other factors include fragmentation, post-blast fire, and building collapse. An estimated 80 percent of deaths in the bombing of the Alfred P. Murrah Federal Building in Oklahoma City were caused by the building collapse rather than the blast itself.

Ultimately, the design of the walls will be an engineering specification. The intent of the design would be to meet a level of protection of Low-Medium-High. These equate to the amount of damage the building will sustain if an explosion occurs nearby. There are cost implications from such a decision, and it is best approached during detailed design. The design recommendations are intended to limit access by potential attackers (vehicle or pedestrian) to the facility

Recommendation

The detailed design should take into account the security requirements of this facility, and the nature of the assets it contains. It is recommended that walls are designed to withstand 2.5 kg of explosive at 10 feet. This is roughly the amount of explosive an attacker would likely use in an IED near the building.

9.1.10 Doors Types

Hollow Core Wood and Glass Doors

Hollow core wood doors and plate glass doors offer little physical security except that the noise of penetrating the glass or the door may deter an intruder. Doors should be constructed to withstand forced entry using impact resistant materials and hardware.

Exterior Doors

Exterior doors should be of solid wood core construction, 45 mm (1-3/4”) thick or be fabricated using 16-gauge metal.

Overhead Doors

Doors with thin wood panels offer poor security. The panels are usually big enough to permit an intruder to crawl through once the panel is removed. Panels can be secured with expanded metal, steel bars or strapped aluminum.

Double Doors

Double doors should have the inactive leaf secured with top and bottom bolts with steel receivers, preferably automatic or edge mounted, unless the doors have a center mullion.

Recommendation

Ensure that door type is relevant to the location and purpose of the door. Exterior doors and doors to secure areas should be the strongest.

9.1.11 Door Frames

Frames and astragals are an important consideration. The door frame should be of good quality construction and match the door construction for strength. To prevent an intruder from spreading the door frame with a pry bar and defeating the lock, the door frame should

be packed with wood or grout. Full length astragals on reverse-hand doors and double-doors offer resistance to prying. Astragals are usually fastened to the door edge with carriage bolts or welded in place. On a double door, the astragal is usually mounted on the active leaf of outward opening doors.

Recommendation

Best Practice should be adhered to. Astrigals should be present on perimeter doors.

9.1.12 Hinges

Exterior doors with hinges on the outside of the door can provide an intruder easy access to a facility. Hinge pins need only be removed for the door to be lifted out of the frame.

Recommendation

Prevent attack by mounting the door on the inside of the frame so the door swings inward, or by installing hinges with non-removable pins, or installing a locking pin in the hinge plate.

9.1.13 Locking Hardware

A wide variety of locking devices and lock hardware is available today. The most common types are listed below:

- Spring-latch locks are beveled-edge spring operated latches that automatically snap into position when the door is closed.
- Dead latches are identical to the spring latch except that when the door is shut the latch is locked by a small pin, offering minimal security.
- Deadbolts do not incorporate a spring function and are usually operated by a key or thumb turn. When properly fitted, this type of lock will withstand most intrusion attempts. A case-hardened steel deadbolt with a 25.4 mm throw will offer adequate security when installed in a high quality door, frame, and wall assembly.
- Magnetic locks should not be considered when local building codes require them to release in the event of a fire alarm. This creates an opportunity for an adversary to penetrate a secure area by simply activating a fire alarm pull station.
- Electronic locks utilize an electric current to activate the locking mechanism requiring an electric strike and hinge set. These typically remain secure during a power interruption without interfering with building egress.
- Keyed locks are needed in almost every application to ensure manual key override.

Keyed locks should be equipped with removable restricted keyway cylinders to facilitate ongoing key and cylinder control. The cylinder, which receives the key, is the heart of the lock. The restricted keyway cylinder determines the size, shape, and complexity of the key. Removable cylinders screw into the lock body and have a rotating safety collar to prevent removal with a vice wrench. A high security cylinder will make the lock resistant to picking, drilling, and brute force attacks. Further, they are not stocked by locksmiths and once installed require special approval by the facility operator before replacement cylinders and duplicate keys are produced by the manufacturer.

Strike plates are used to protect the lock bolt and add strength to the lock bolt receiver. A wrap-around strike plate or strike box will provide even greater strength.

Recommendation

Ensure that all keyed locks include high security cylinders.

9.2 Security Systems

9.2.1 Integration

Electronic security systems should be designed and installed with deliberate consideration for their ultimate goals. Security systems should be integrated seamlessly with each other, allowing a simple and effective user understanding and response to critical situations identified by the systems.

Integration is a central tenet of modern security design. Proper integration provides the end user with a greatly enhanced security capability, leading to a much higher level of comfort for the personnel that are protected by the system. Additionally, effective integration reduces training costs, limits maintenance costs, enhances the ability to quickly troubleshoot a system, and provides a notably more effective response from security personnel.

Integration is the interaction and sharing of information, features, and functionality between systems and people in order to effectively and efficiently perform a function. Strong integration will reduce the amount of interaction required between technology and people, which has two key benefits – the freeing up of personnel resources to perform other functions, and the reduction in possible points of failure in a system.

Conventional contracting methods in security usually end up with several systems from several different vendors, each supplying a different component of the system. While a certain amount of this is inevitable, it can create extra cost for the owner in the areas of training, installation, and maintenance. Developing a commonality in the systems under design is now the preferred choice. This commonality is a methodology by which differing components can function as one, reporting through the same interface to an operator.

The advantages to the user are several. Functionally—this requires the operator to learn only one interface while operating multiple systems (e.g., CCTV, intrusion detection, access control, fire, HVAC, etc.); therefore, the cost of training is thus reduced. Additionally, training or re-training processes on a single system is significantly easier and less costly than specialized training on each of the systems that are to be monitored.

The integrated approach also allows the use of a single workstation for the monitoring personnel, as opposed to the need for multiple computers and workstations for separate systems. The savings are not just in the cost of the extra computers, GUI's, and peripheral devices, but also in actual real estate (space), which can be used for other things.

Recommendation

Design of all security systems will require full integration of the various security components.

9.2.2 Access Control System

The access control system will be the managing component of the entire security system. All gates should be equipped with a card access system to control entry and egress. Each building or structure, as well as high priority areas within buildings, also should be equipped with card access at a minimum of one entry point. High priority assets should be protected with access control requiring something in addition to a card, such as a PIN or biometrics.

An access control system provides a wealth of information that relates to both safety and security. The system should be able to provide reports that can be used as an investigative tool. The following matters, all of which can be determined via the software, should always be investigated:

- Propped doors;
- Cards read in unauthorized areas;
- Cards read at unauthorized times; and
- Compliance with entry/exit procedures at gates.

The last point above relates to the problem of personnel not always properly carding into the site. For example, when carpooling, there are often times when only the driver will read their card to gain entry, no one else will. This creates both security and safety issues, as no one can be sure who is on-site.

Card access systems provide access via authentication (e.g., an access card) and authorization (where a given card is accepted). Authorization links authenticated individuals to the specific buildings or areas to which they are entitled to have access by establishing rules for each controlled access point. The authorization process is rightly in the hands of the access-system administrator and management.

Authenticity can be provided via three factors:

- Something you have (a card, a key);
- Something you know (a PIN number); and/or
- Something you are (biometrics).

The more factors required, the better the security. At the same time, there is a need to balance security requirements with operational efficiency. For the most part, using a card (something you have) as single factor authentication is strong enough security; however, for high priority assets, multiple-factor authentications should be used.

Recommendation

Vehicle ingress and egress gates for IROC secured parking areas are to be card access controlled. Public vehicle entry is not. Where there is a need to provide public access to the IROC facility (as required by several stakeholders) this open access will be to a contained reception area. Any movement beyond the reception area will require the use of the access control system. Inside the secure area, certain areas will be designated for higher levels of control. These areas are to be administered by whoever is responsible for administration of the access system. Finally, highly critical areas such as the server/communications rooms will be provided with two or three level authentication procedures. The server room will

function as a collocated room for equipment from all stakeholders, with each stakeholder having secure access to their equipment, within a secure room.

9.2.3 Intrusion Detection and Alarm System

The entire length of the perimeter should be equipped with intrusion detection devices that are integrated into the alarm system. All entry points into critical buildings and structures, including windows and roof hatches, as well as high priority areas within buildings, should be monitored as well.

Use of perimeter alarming will provide early warning of an intruder, be they malevolent or accidental. By integrating the perimeter alarming to a CCTV system, the capability will exist to ensure that there are a limited number of nuisance alarms, and that alarms are properly verified prior to response. Within the building itself, alarm devices will provide notification of entry to secure areas.

Sensing devices are connected to the controller by hard-wired circuits or radio frequency transmissions. Many types of sensors are available—most systems use some combination of the following:

- Magnetic contacts (also known as dry contacts) are used on doors and windows sending their signal when the circuit between the contacts is opened.
- Motion detectors detect *movement* using many different technologies, (e.g., passive infrared, ultrasonic, microwave, infrared beam or 'dual technology' detectors that combine more than one of the above).
- Foil tape is applied to the interior surfaces of glass windows or doors, and alarm when the glass breaks the foil circuit.
- Acoustic glass break detectors are designed to recognize changes in acoustic (sound) frequencies (at 3-5 Khz range) caused by breaking glass.
- Vibration Detectors are closely related to the glass break detectors and recognize seismic vibrations (at 200 Hz) that occur when an intrusion occurs.

Recommendation

The perimeter is to be alarmed with a combination of technologies, depending on the eventual construction design (CMU Wall, chain link fence, minimal perimeter). All the perimeter alarms will be verified by the integrated CCTV system. Within the building itself, all perimeter entry points (doors, windows, hatches) will be monitored by appropriate devices. Each of these devices will report exact location and type of alarm to the control system. Where possible, verification will be provided to all alarms via CCTV. Certain areas within the facility, such as the server room, will be provided with a higher level of alarming, typically meaning more devices as an intruder moves through the area.

9.2.4 Closed-Circuit Television System

CCTV should be used for four purposes: alarming, assessment, surveillance, and investigation. The entire length of the perimeter, clear zones, and high priority assets should be monitored by video surveillance. A combination of PTZ and fixed cameras should be used as necessary to provide the best possible coverage. The system should have a sophisticated digital video management system capable of Geographic Information System

(GIS) integration, camera control, video distribution and analysis, sensor integration, and alarm notification.

The CCTV component of the security plan should be viewed as an entire system that is greater than the sum of its parts. It is important not to attempt to consider the cameras separate from the security management system, nor the reverse.

Video cameras now have the capability to note motion in their field of view by several different technologies and can trigger an alarm situation when that occurs; however, camera motion detection should not be relied on as the primary or sole detection system as there should be other detection systems in use as well. CCTV cameras should also be used to provide assessment when another detection system creates an alarm. They should also be capable of filling a general surveillance role, being used for pre-programmed tours of the compound when not responding to alarms. Finally, the system should provide a high degree of investigative capability, with easy retrieval of stored video and assurance that the video was not tampered with, in the event that it is ever required as evidence.

The system of cameras should include a combination of PTZ and fixed cameras. The PTZ cameras should be used for overwatch and alarm assessment, while the fixed cameras should be responsible for alarm assessment, general surveillance, and in some cases, alarm detection.

It is noted there are several cameras that are part of the ISP campus. Where it is appropriate to do so, these can be incorporated into the new system, assuming ISP is interested in doing so. The nearby CCTV can be useful, and should be incorporated into security at this facility; however, at no time should a security system for a site such as this be relying on an outside system for primary information. If you do not control all aspects of a component (installation, control, maintenance, programming, etc.) it cannot be relied on as primary source information. It is very useful as a complementary system.

Digital Video Management System

The Digital Video Management System (DVMS) should provide a distributed, scaleable set of technologies for detection, transmission, and notification of alarm events. The fundamental objectives of the technology are to be able to easily integrate with standard devices and sensors in the field, process the information from the devices, derive alarms based on significant changes in the devices' state, and then annunciate the alarm through a set of open interfaces. This will require open architecture at the head end of the system so it can be easily integrated beneath more sophisticated command and control software.

In particular, the system should include a suite of technologies for managing and analyzing digital video, controlling cameras, and interfacing to the perimeter intrusion detection system. The DVMS should be capable of working with a large number of different manufacturers' PTZ cameras.

Camera and DVMS Selection

The camera selection process is simplified because at this point in the evolution of the video security industry, cameras from most of the major manufacturers (Panasonic, Sony, Sanyo, Phillips, Silent Witness, Vicon, Pelco, and several others) are very similar in their capabilities. The optics are generally excellent from these major manufacturers, and selecting almost any one of these should satisfy the minimum requirements.

In making a selection of the CCTV product, the following factors should be considered:

- Manufacturer support;
- GIS integration;
- Camera control;
- Video distribution;
- Video analysis;
- Sensor integration; and
- Alarm notification.

Geographic Information System Integration

The use of mapping technology to locate and position devices, cameras, and alarms within the real world provides several benefits, in particular for large outdoor areas to be monitored. In the case of IROC, the size of the tract of land and the footprint of the building will determine the level of value that GIS integration brings.

The system should be able to associate latitude and longitude coordinates with every object and alarm it manages. This allows the production of map displays of the location of devices, cameras, and alarms. The map displays can incorporate industry-standard GIS data files, such as aerial photographs, street names, critical building locations, etc. Users can zoom or pan maps to any level, and they can interact with the objects represented on the map. For example, clicking on a camera icon immediately causes video to be displayed from the corresponding camera. These capabilities allow the operator to spatially associate and navigate video and alarm data and their locations in an intuitive manner, without requiring any special user interface programming on the part of the system integrator. GIS mapping capability would certainly provide a very high level of situational awareness for the operator.

An additional benefit of having a native GIS capability is that the DVMS could then automatically relate the sources of events with a means to evaluate or corroborate them. For example, if the system knows where each camera is and can determine where an alarm from a fence intrusion system is occurring, it can automatically position PTZ cameras to look directly at the point of intrusion without requiring any camera preset programming or relay contacts between the camera and the fence. In the case of a large perimeter, this feature can save hundreds of hours of system integration time because the entire automated video surveillance response along a perimeter can be configured from a simple drawing that might take a few hours to produce. Again, the eventual size of the site will determine the utility of this feature.

Camera Control

An important part of site surveillance is corroboration and assessment of alarm conditions. The use of PTZ video cameras is an efficient way to provide alarm assessment prior to response being dispatched. Automating the control of PTZ cameras reduces both the time required to perform an assessment, and the skill required of a human operator to track an object interactively. The two key capabilities of high-end camera control software are:

- Providing remote-control techniques that drastically reduce the effect of latency and bandwidth on camera positioning; and

- Using native GIS capabilities. This increased level of situational awareness will increase the capabilities of the monitoring personnel.

Typical joystick camera control presents problems to operators when used with digital video. The problem is that the up/down, left/right, in/out control actions are all "relative" positioning commands. The operator depends on feedback from the video to determine when to stop moving the camera. If there is enough latency in the video feed (due to bandwidth limitations or streaming compression characteristics) then the operator will consistently overshoot their target. The problem is compounded if the operator is trying to track a moving target.

If the DVMS can position outdoor cameras using absolute coordinates, it would be able to support an alternate camera control methodology. Instead of moving the camera left/right or up/down, the operator would simply click on a spot on the video image where they would like to camera to point. The camera would automatically move so that this point becomes the center of its field of view. Within the constraints of the camera's optics, the camera should automatically position and zoom to match the operator's request. This point-and-click camera control capability would greatly reduce the effects of video latency and increase the ability of an operator to track a moving object, while reducing the manual dexterity required to do so.

Another advanced feature of modern camera control technology is the ability to automatically direct a PTZ camera to track one or more objects in its field of view in an outdoor environment. The advantage of this is two-fold: it drastically reduces the need for a human operator to control the position of a camera, and because the control technology is based in an independent processor, it is independent of camera make and model.

Video Distribution

The DVMS should provide centralized access to all remote video camera feeds through a central server, eliminating the need for the user to figure out which remote device needs to be accessed in order to get video from a camera. Video should be distributed using standard Internet Protocol (IP) networking protocols, so that it is available to any device that has an IP network connection, including web browsers and handheld devices. This capability can be important during a manned response to an alarm, where the responder can quickly view and take control of a PTZ camera before entering the subject location.

Standard MJPEG compression technology reduces the bandwidth required to transmit live video. The use of MJPEG compression results in very high quality video images, at the expense of slightly larger image sizes than, for example, MPEG4 compression. Furthermore, because MJPEG compression does not attempt to compress information between video frames, there is no latency due to compression in the video feed. This means that the network bandwidth would be the only source of latency between a user and their view of "live" video. This is particularly practical for users that rely on live video for feedback when controlling a remote PTZ camera. The more latency that exists between the controller and the live video images, the more the position of the camera will overshoot.

Video Analysis

Most digital video recorder (DVR) manufacturers include some variety of video motion detection algorithms in their camera or DVR. Typically, these algorithms work well in

indoor environments or where lighting conditions are carefully controlled. Because the IROC project will include perimeter surveillance and alarming, there is a need to have the video processing and the motion detection function in the various lighting and weather conditions experienced in the outdoors.

Sensor Integration

The DVMS should be capable of integrating with third-party devices through dry-contact relay in/out, RS-232/RS-422/RS-485 serial communications, and ethernet. The information provided by these devices can be used to generate alarm conditions, turn on programmed camera motion detection configurations, move one or more cameras to specified locations, or send a control signal to another type of device.

Alarm Notification

The alarm notification system should be sophisticated and flexible in order to distribute alarm information both to monitoring personnel and to other systems.

Alarm enunciation should be available through e-mail, pagers, and voice telephone calls. In addition, there should be a graphical map-based console to provide operators with an intuitive view of a system by incorporating aerial photographs and other geographical contexts for alarms and video display.

The notification system is intended to let users define a contact hierarchy, where each individual has designated methods of contact and a schedule for contact. The methods for contact may include e-mail, pager, voice telephone call, or any other contact method plug-in the system integrator supplies. The contact schedule specifies rules for when each contact method may be used, along with exceptions to those rules. Contacts can subscribe to different alarms either globally or on a per-site basis. More than one contact may subscribe to the same alarm. Each level in the hierarchy has a defined emergency contact that will be used if a designated contact for an alarm cannot be successfully reached.

Each contact action taken for an alarm should be logged, along with an indication of acknowledgement.

Recommendation

The security design for IROC is to include CCTV coverage of the entire perimeter and all parking areas. These cameras will provide secondary alarming capability, alarm verification, and surveillance. Within the building, the reception area will be under surveillance by CCTV—which in fact is a safety measure as well as a security measure. High security areas (servers, communications) interior to the building will have CCTV.

All CCTV will include software intelligence to provide alarming and other functions noted above. All CCTV will be available as necessary by the administrator to any person who is deemed to have access to the video. This video will be distributed by multiple technologies, as agreed during the design phase of the project. All video is to include watermarking or other accepted identification techniques to ensure continuity of evidence in the video.

9.3 Security Policy and Procedures

Corporate security policy is the high-level plan by which senior management expresses its commitment, delegates responsibility, establishes standards, and sanctions certain activities to protect the organization and its assets from harm.

Documented security policy and procedures aid in creating a culture of safety and security throughout the facility and organization. Security procedures describe the functionally relevant security activities to be undertaken by employees performing their day-to-day work. They are instrumental in guiding employee behavior with respect to personal safety and security and in providing them with the information, tools, and support needed to act appropriately in the event of a threat. Some security procedures would have organization-wide application, while others would be site- or department-specific. All procedures that are in use should be available to all employees. Typically this can be done via an internal web site.

Recommendation

IROC will incorporate multiple agencies. Most of these agencies will already have local security policy. It is critical that IROC develop its own security policies and procedures—unique to the staffing and operation of the facility. The documented security policy that is approved by senior management of all participants, will be readily available to all persons working at the IROC facility, and will be subject to periodic review and revision by management. Revisions to the document should be published, communicated, and distributed to all personnel, accompanied by a revision checklist.

The IROC facility should have documented procedures governing the subjects listed below. These procedures are detailed step-by-step actions to achieve a certain task. They should explain clearly how policy guidelines will be implemented in the operating environment.

The policy should speak to a number of procedural issues, including:

- Background checks;
- Photo identification badging;
- Key and access card control;
- Deprovisioning;
- Contractors;
- Visitors;
- Access and pedestrian flow;
- Incident reporting;
- Records management;
- Change control;
- Training and awareness;
- Performance measurement;
- Security continuity of operations;
- Fire drills;
- Bomb threats;
- Emergency planning; and
- Delegation and authorization.

9.3.1 Background Checks

Background checks should be performed on all employees, regular contractors, and vendors to reduce the risk of hiring or allowing access to a potentially dangerous person.

Criminal record background checks should include a combination of local, state, national, and international checks that depend on the position and access that the applicant will have within the facility. Furthermore, persons in positions of trust should also have checks done on credit, fraud, and education. It is not unusual for persons to misrepresent themselves when trying to obtain a new position. This is very often a dicey issue for Human Resources personnel; however, the post-9/11 world dictates new requirements, both legislated and common sense. Despite best efforts, it is clear that employers do not always know exactly whom it is they are hiring. As the liability moves increasingly toward the employer for incidents that occur within the workplace, the more information obtained on personnel, the better for both safety and security.

Recommendation

The various partners in IROC all have differing background check requirements within their own agencies; however, as with the rest of the security program, the availability of confidential information at this facility requires that a high standard be maintained. Discussions with ISP in particular highlight the fact that if persons without the proper clearance were allowed near any future ISP stations in the facility, ISP could conceivably lose access to some national intelligence and police databases. As a result, all participants have agreed to modify their background check requirements for their personnel that will have access to the operations floor in IROC that will meet the minimum standard of no felony convictions on record. This is consistent with the requirements of the most secure potential agency to be collocated in the future.

9.3.2 Photo Identification Badging

Staff within the facility should be able to readily identify other staff, contractors, or visitors via photo identification badging. Employees and contractors issued badges should be subject to background checks and should be required to sign an acknowledgement of the conditions of use for the badge. Contractor badges should have an automatic expiration date.

Whenever a badge is provided, to either an employee or a contractor, the receiver should be required to sign an acknowledgement of the conditions of use for the badge – matters such as not loaning the badge, reporting it when lost or stolen, and using it only for authorized purposes.

Recommendation

All persons using the IROC facility will be required to have and display a photo identification badge, to be controlled and distributed by IROC management. The staff badges will be visibly different from contractor or visitor badges, and if warranted can be color coded for certain high security areas.

9.3.3 Key and Access Card Control

All keys and access cards that allow perimeter entry or access to restricted or critical areas should be controlled and stored in a secure manner. Keys should be issued only to those persons who can be entrusted with them and who have a legitimate and ongoing need to access secure venues.

Key issue records, key control cabinets, key inventory audits, and master key control are necessary ingredients in an effective key control program. Key and access card control can be maintained several ways. The least efficient but most common method is the key log, typically a pen-and-paper exercise whereby all keys are centrally stored and signed out on an as-needed basis. The required personnel resources for this function are what generally make it the first gap in the security system. In short, it is too time consuming to expect key control to be maintained in this way. Rather, there are automated systems that can control access to keys and access cards and maintain tight control, to the benefit of the security profile.

IROC is at a certain advantage, in that this is a brand new facility, and positive key control can be planned and maintained from the outset.

Recommendation

The issuing of long-term use keys and access cards to new users should be regulated and all such items properly logged. As with the identification badges, all recipients of keys and access cards should fully understand their appropriate use, that duplication is prohibited, and also sign an acknowledgement of the terms and conditions of their use. An automated key control and inventory system should be implemented to assist in the control function.

9.3.4 Deprovisioning

All departing employees should be required to complete a deprovisioning process that includes return of all organization equipment, including keys and access cards. All members of the staff should be promptly informed of any departures.

If a former employee still has keys or access cards to the facility, the site and everyone in it become vulnerable to the key holder. Re-keying locks is far more expensive than recovering keys when a person leaves. Furthermore, it is essential that all personnel be informed of employee departures to ensure that everyone is aware who is authorized on-site.

Recommendation

IROC should meet the Best Practice standard described above.

9.3.5 Contractors

Contractors should be issued badges, which should have an automatic expiration date. They should be subject to background checks in order to receive their badges, and they should be required to sign an acknowledgement of the conditions of use for the badge. Unless a contractor has undergone the requisite background check, escorts should be mandatory.

Recommendation

Contractors who are long-term should be issued badges after a background check, which may provide them access to secure areas. Periodic audits are necessary to ensure badges are not being passed around among contractors. Short-term contractors are to be treated as visitors.

9.3.6 Visitors

All visitors should sign in at the main facility entrance where they should be issued visitor badges. Sign-in should require a government-issued photo identification. The employee the visitor is meeting should be notified. All visitors to the site should be escorted at all times.

Recommendation

There should be no deviation from the Best Practice described above. At no time should visitors be unescorted within the facility.

9.3.7 Access and Pedestrian Traffic Flow

Perimeter access to the facility should be limited to as few locations as possible, and each access location should be equipped with a monitoring device. Physical barriers and electronic technology should exist to impede intruder traffic flow or monitor it throughout the facility. Critical buildings should be locked at all times, with audited card access controlling entry.

Recommendation

The facility should be divided into four security zones.

- The public/reception zone is that area to which the general public has unimpeded access during normal business hours. It will be constructed and equipped to prevent unauthorized entry to the remaining portions of the building.
- The administrative zone(s) are those that accommodate administrative assets and activities and may include the common-use areas (i.e., lunch, locker, and wash rooms). This zone will be physically partitioned from the other zones.
- The operations zone(s) are those that accommodate assets and activities of an operational nature, (i.e., communications centers) and will be physically partitioned from the other zones.
- The secure zone(s) are those that contain high criticality assets or activities, (i.e., IT network and data server rooms, telecommunications closets, electrical/mechanical/ HVAC compartments).

9.3.8 Incident Reporting

An organization should have a system available for proper and effective reporting and tracking of various types of incidents at the facility.

Having a proper incident reporting system that is easy to use and readily available should increase the likelihood of employees reporting matters that directly or indirectly affect the safety and security of the site.

Recommendation

IROC should develop a reporting tool unique to the facility to encompass security notifications as well as other features, such as maintenance requests.

9.3.9 Records Management

All records should be placed in a classification system and access to them should be governed according to this classification. Access to records should be role-based and should be at the discretion of the owner of the records. Computer systems should be protected against external hackers by firewall technology and against unauthorized internal access by authentication verification software.

Recommendation

Each agency will have its own Records Management policy. As no participant will be keeping controlled or confidential documents on-site, there would be no need for the stakeholders to have a separate policy or procedure.

9.3.10 Change Control

Change-control procedures pertaining to the automated security systems should be developed and documented.

Change control is an integral part of any business process. As far as the security systems are concerned, any changes to cards, locks, cameras, or alarms should be required to have managerial approval. There should be an audit trail of these requests and approvals. Once the manager requests the change, the appropriate administrator should provide the required cards or changes. Change control should also include an audit process.

Recommendation

Changes to the physical layout or the electronic security system should be requested in writing and the changes documented. These changes include items that may appear to fall under the radar, such as a change in the time that the intrusion system disarms, for instance. Any changes should be communicated to all users.

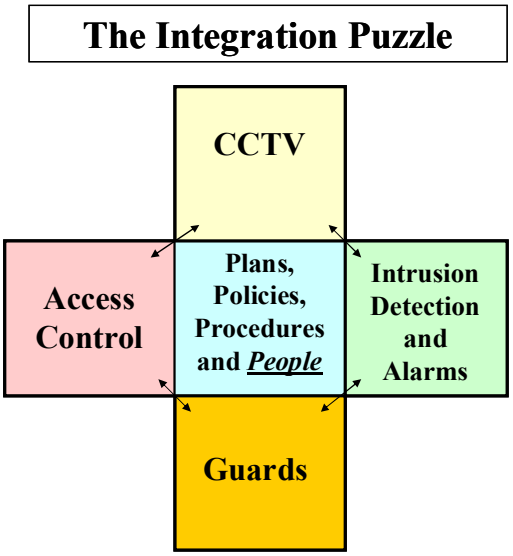
9.3.11 Security Awareness Training

Regular training sessions should be delivered in various formats to ensure that the staff is aware of their security responsibilities, and to provide staff with the proper methodology to meet these responsibilities.

A critical component of any successful security plan is making sure those involved in the plan understand that security is everyone's responsibility. A security practitioner can design an ideal and appropriate system, but if the users see these measures as an inconvenience rather than a benefit, they can and will compromise the system; therefore, training and awareness are vital components of the security profile of a facility.

The Integration Puzzle, shown below demonstrates the entities that need to be integrated in order for the security system to be successful. Far too often, technology solutions are relied on for the entire security profile. When integration is discussed in the security industry,

generally it is about the integration of CCTV and access control, of intrusion detection and CCTV, and between different building management systems; however, the key piece in the Integration Puzzle, which is often neglected, is how personnel integrate with these other systems. If they do not fully understand the reasoning behind the security, if they do not understand how the systems are intended to function or why, if they do not take an active role in the security plan, then the rest, unfortunately, is for naught. The presence of policies, procedures, electronic security systems and contract guard forces is irrelevant if the facility users are not properly informed and included as part of the security solution. With the advancement of technology, training has become a more important aspect of the ever-changing business environment.



An organization's first line of defense is its employee population. The intent of security awareness training is to utilize all employees as eyes and ears to protect the assets on-site, including other workers. Training is the formal procedure that an organization utilizes to facilitate personnel learning so that the resultant behavior contributes to the attainment of the organization's goals. If employees are not properly trained in security procedures, and if there is no compliance auditing in place, it is an uphill battle to have the employees comply with the security program. In that case, the security systems are often seen as a hindrance and an inconvenience, and accordingly they are overridden wherever possible.

When a security program is designed organization-wide, it can impact the different functional groups or facilities of the organization in different ways. When that is the situation, the responsibility for creating security awareness should be delegated to the level of the facility manager.

The effectiveness of a security awareness program depends on the purposes for which it was originally developed. These purposes allow each employee to:

- Understand the relationship between security and successful operations;
- Know his/her own personal obligations under the security program;
- Perceive the connection between security program objectives and selected security measures;

- Be familiar with sources of help in carrying out personal and departmental responsibilities under the security program;
- Comply with statutory or regulatory requirements; and
- Comply with contractual obligations.

The long-term payback of such a program makes the capital investment in the security infrastructure far more valuable, and far more beneficial.

Recommendation

All regular users of the IROC facility should be provided with a short, one hour indoctrination into the security program that will be in place at the facility. This includes a description of the systems, as well as the procedures necessary to provide a secure environment.

9.3.12 Systems Training

Beyond security awareness training comes the matter of systems training. There are three levels of training required on security systems. The first level is for persons who are operating and monitoring the systems, and this level can be provided on-site by the integrator, the vendor, or an independent consultant with training expertise in security. The second level of training is intended to reach system administrators, and provides information on how to organize and run the system. This level of training is most often provided at the factory, and depending on the system would be a one to three day course. The third level of training is system maintenance. This training is provided to give the owner the ability to maintain the system on a day-to-day basis, to trouble shoot minor problems, and to identify major problems. Actual repair of major problems should be part of an extended warranty or on-call repair program. Maintenance training requires some knowledge of electrical systems, and is generally delivered on-site by the integrator and vendor to qualified personnel.

Recommendation

Specifications on the eventual security system should include the training requirements provided above. The specification should ensure that the syllabus is provided in advance, and that the trainers provide qualifications and references.

9.3.13 Performance Measurement

All elements of the security program should be audited regularly against a baseline performance. This applies to physical, electronic, and procedural security.

Recommendation

The Best Practice described above is appropriate for this facility.

9.3.14 Security Continuity of Operations

There should be a contingency plan to maintain the security profile of the facility in the event that one or more security components become inoperable.

The security profile can become compromised if any of the physical security devices or security systems becomes damaged or fails to operate. Failure can occur for any number of reasons, including power outage, fire, natural disaster, or accident. Until the system can be repaired or becomes functional once again, measures should be taken to patch the gap in the security profile. For example, if an errant vehicle were to crash through a perimeter fence, a guard stationed at that location until the fence can be repaired could protect the hole in the perimeter.

Recommendation

IROC should develop a written plan that is essentially part of the Business Continuity process. It should be tested and evaluated on an annual basis.

9.3.15 Security System Monitoring

Security systems should be monitored around the clock by adequately trained personnel. Ideally, monitoring should be performed simultaneously by guards on-site and by other organization personnel at an off-site location specifically designated for security operations.

Effective monitoring of the security system is possibly one of the most critical elements of the entire security plan. Without an effective monitoring component, the entire system is rendered useless because it becomes very easy to compromise. Unmonitored alarms result in a lack of response to those alarms, which in turn results in a lack of confidence in the system. Sporadic or complete lack of monitoring can lead to an event being discovered only after it is too late to intervene or limit damage.

A security system loses a huge amount of its capabilities if it is not monitored correctly. Real-time monitoring of the system provides an organization the ability to detect an incursion, assess it promptly and properly, and respond to it in an appropriate and immediate fashion. The monitoring personnel are advised of a breach in the security profile. They use tools to assess the breach, and they can then send the contract security or other personnel to respond. If the assessment indicates a false or nuisance alarm, it can be ignored.

Monitoring should also be undertaken for investigative purposes. The access control system, in particular, provides a wealth of information that should be utilized as fully as possible. As an example, the system pinpoints occasions when a card holder has used his/her card to attempt to access a restricted area. If this occurs one time, it could be happenstance, but pattern of these occurrences could indicate a serious problem. Only with proper monitoring and auditing of the system can a pattern to inappropriate usage of cards be detected. This is just one of many ways that monitoring for investigative purposes can be employed.

Simultaneous monitoring by on-site and off-site personnel should be used in order to provide redundancy. Furthermore, monitoring on-site and off-site each has its own advantages, so using a combination of both provides the maximum benefits. Monitoring stations, both on-site and off-site, should be equipped with the ability to monitor all security system components. Personnel tasked with security functions have been shown to be far more alert, efficient, and productive when provided with a fully equipped monitoring station. Furthermore, monitoring personnel should be situated at a console that is dedicated to security monitoring, and they should not have other duties that could preclude effective

and constant vigilance. Regardless, the system should have the capability to notify persons away from this console of alarms.

On-Site Monitoring

The primary benefit of having on-site personnel monitoring the system is that response can be immediate. The best on-site personnel to monitor the security system are the facility's guard force, where such a force exists. The alternative to the guard force is operations personnel. Although operations personnel are often better-trained than the guard force, they are usually preoccupied with other duties. The main task of operations personnel is to monitor processes within the facility, and when a network or process situation arises, it often takes precedence over security situations for those personnel. It is very common for security alarms to be completely ignored in order to deal with a process crisis. On the other hand, security guards have one job, and one job alone: security. Relying on operational personnel to monitor the security systems could seriously compromise the security of the site.

Adding the monitoring function to guard duties does not overly burden the guards. The security systems are designed to be operated and understood by security personnel. They are extremely intuitive and provide internal help functions and direction. The integrator and/or manufacturer should supply comprehensive training at the outset, followed by refresher training on a periodic basis to keep guard personnel familiar with the systems. Because these personnel work with the systems on a regular basis, they do not fall out of practice. Plus the presence of well written procedural manuals certainly helps. Experience has shown that a well trained contract guard can in fact effectively operate these systems and provide the necessary on-site monitoring. Any breakdown typically occurs if the training and procedures are not clear enough.

The on-site monitoring station or stations could be located in the guard houses at the gates of a facility. Those stations should provide access to all alarms from the system. Using the integrated tools at the station, the gate guards are able to assess and respond to any security situation. Additionally, the technology exists to have guards on patrol have access to video alarming and control, and this capability should be integrated into the system design.

A standard design to an on-site monitoring system includes administration rights only as necessary for the guards. The guards typically should not have control over most of the administrative functions of any of the systems, including such issues as camera set up, card activation or production, and alarm set-up. If the guards are the only monitors of the system, they need to be able to activate or deactivate intrusion systems to accommodate authorized contractors after-hours. They also need the capability to control all doors and gates remotely, once again to ensure that security functions do not make operations impossible to achieve; however, clear direction in policy and procedure as well as proper initial set up ensures that they have all the possible functions they require, without the ability to change the system in any way that could compromise security. In any event, it is critical that audit logs are produced by all systems to indicate who has used them, when, what the systems were used for, and what changes, if any, were made. The ability to fully audit all usage allows the administrator to fully track and investigate any issues that may arise.

Off-Site Monitoring

In addition to on-site monitoring, there should also be an off-site monitoring station that, like the on-site stations, has the ability to monitor all activity on the system. Personnel at that central station should be dedicated security monitoring personnel who are well trained on the systems and have a security background. Training and deployment of appropriate procedures for these personnel is absolutely essential.

There are several advantages of off-site monitoring. First, there is detached automatic response to all alarms, regardless of any internal or personnel issues that may hinder on-site monitoring. Also, the off-site monitoring station can provide regular reports, can notify plant personnel as required under operational procedures, and can be instructed to notify other off-site organization personnel as well for certain alarm types. Additionally, they can ensure response from the on-site guards and report on the speed and quality of that response. The only operational downside to off-site monitoring is the lag time between alarm, notification, and response. It requires human interaction, and can take longer than an on-site monitored response; therefore, it works best in combination with on-site monitoring.

There are two primary options for off-site monitoring: having a station controlled and run by personnel directly affiliated with the organization, or outsourcing the monitoring to a professional monitoring company.

The main benefit of outsourcing is that the responsibility and management of the monitoring function, including installation of monitoring equipment, testing, and maintenance, are contractually handed off to a third-party. This eliminates administrative overhead; however, a large degree of control is still maintained, as the third-party monitor operates only on instructions provided by the organization that runs the water facility. However, outsourcing monitoring to a third-party requires monthly operational financial costs, which are based on the size of the security system. Furthermore, it is not uncommon for third-party monitoring sites to actually be located elsewhere on the continent, and to be using long distance via either phone or wide-area network to perform the monitoring functions. This is not an optimal scenario for both operational reasons (e.g., time lag) and administrative reasons. When third-party monitoring is used, the selection should be of a station located in the same metropolitan area as the water facility.

Recommendation

IROC should resource for on-site security forces. These personnel would be responsible for investigation and preliminary verification of alarms. They would also be the first responders for most events, and the conduit to emergency services for more critical events. The security force should be located within the building itself. If the ISP campus area is chosen for this facility, it may prove useful to share monitoring of systems with ISP.

9.4 Preventative Maintenance

All electronic systems should have regularly scheduled preventative maintenance programs. The owner should require detailed reporting of the program.

A security system, as with any other electronic system, requires regular maintenance. The system is composed of electronic and mechanical parts, each with a mean time to repair that should be observed. Failure of any one component of the system can compromise the entire system and the

security of everyone and everything that it protects. An electronic security system that is not maintained on a regular basis will soon fall into disrepair and will not provide the function it is designed for, ultimately costing the organization significant outlays of capital.

Maintenance should be performed on a scheduled basis. Twice a year is usually frequent enough to maintain any of the systems considered on this project. Some portions of the system (e.g., camera views at the gates) will need more frequent attention. The maintenance would include matters such as cleaning and adjusting cameras, testing preset locations on PTZ cameras, and fine-tuning and recalibrating fence alarms. A full preventative maintenance package would be detailed in the final specifications for the system. The system integrator would be capable of providing this twice-yearly program; however, site personnel could be trained for it as well. The critical matter is to ensure that, no matter who is responsible, it is done on a schedule and maintenance records are kept on file.

Recommendation

IROC should include in the security specifications the requirement for a long-term preventative maintenance program at the facility.

10. SUMMARY OF RECOMMENDATIONS AND FINDINGS

Numerous strategic and tactical recommendations are made throughout this report and are summarized in the following sections.

10.1 Findings

- Candidate locations 1, 2, 4, and 5 were near-equal in their respective National Cap Index Scores of 51 and 52. Candidate location 4 had the lowest National Cap Index Score of 47; however, none of these scores are particularly high in the broader scope when compared to national figures.
- Current analysis of terrorist goals and motivations points to domestic and international critical infrastructure and key resources as potential targets for terrorist attacks. A disturbing trend is the networking of terrorist, extremist and transnational organized crime groups.
- Terrorist and extremist groups are actively searching the Internet to acquire information and capabilities for chemical, biological, radiological, and even nuclear attacks.
- Organized crime groups continue to pose a primary threat to public safety and security. There is a growing recognition that like terrorist groups, organized crime is shifting toward fluid network structures from their formal hierarchies.
- Amateur, opportunistic criminals (both insiders and outsiders) continue to take advantage of low-risk opportunities to perpetrate the majority of their crimes utilizing over a dozen potential attack vectors.
- Fire is a greater and more probable threat than crime. Modern communications and data centers undergo enormous pressure during crisis events. Fires inside these types of facilities are caused by electrical faults in raceways, cable trays, beneath raised floors and inside other concealed areas.
- The frequency of natural disaster events and costs associated with responding to them are both expected to continue to trend upward.
- Cyber-threats represent a very real danger to government and more particularly, to law enforcement and intelligence operations.

- Incidents of violence in the workplace are becoming widespread, and in the interests of public safety, organizations must be more vigilant in anticipating and protecting against such incidents.

10.2 Strategic Recommendations

- Given its value, sensitivity, and criticality, IROC is recommended to be situated at either of the two candidate locations adjacent to the ISP campus or the I-84/Meridian Road interchange. Considering the proximity of all potential sites, the risk from international terrorism, internal terrorism, organized crime, and internal (employee) issues does vary among sites. A motivated, prepared attacker will not be deterred b y the space of a few blocks travel. However, other factors also have effect. The traffic and zoning issues have been discussed in this document, each of which point to the ISP campus area as the best choice of those available. Additionally, as discussed the ISP campus area provides several advantages to the facility:
  - Quicker response to major incidents;
  - Sharing of local physical resources (human and electronic); and
  - Proximity of the ISP should provide a deterrent from non-professional crime..
- The value, sensitivity, and criticality of the assets under protection at this facility require that IROC should be treated as a high-security venue. Accordingly, security design should conform to “Best Practices” detailed in this document.
- The facility should be divided into four security zones.
  - The public/reception zone is that area to which the general public has unimpeded access during normal business hours. It will be constructed and equipped to prevent unauthorized entry to the remaining portions of the building.
  - The administrative zone(s) are those that accommodate administrative assets and activities and may include the common-use areas (i.e., lunch, locker, and wash rooms). This zone will be physically partitioned from the other zones.
  - The operations zone(s) are those that accommodate assets and activities of an operational nature, (i.e., communications centers) and will be physically partitioned from the other zones.
  - The secure zone(s) are those that contain high criticality assets or activities, (i.e., IT network and data server rooms, telecommunications closets, electrical/mechanical/HVAC compartments).
- Security should comprise physical, logical, and electronic components. The electronic systems should be integrated, reporting to a dedicated security monitoring position within the IROC facility. The electronic systems should report to an on-site security force, with the capability for off-site monitoring as well.
- Security policy and procedures will be needed to support the other components and ensure the achievement of the security objectives.
- Emergency Preparedness, Disaster Recovery, and Business Continuity Plans are necessary, and should be integrated with the security policy and procedures to ensure that the facility is protected from a disruption that would render it ineffective.

10.3 Tactical Recommendations

Type Key:
P = Physical Security
A= Administrative, Operational, Maintenance Issues

Design Feature	Type	Design Recommendation
Stand Off Zones	P	▪ Demark a perimeter barrier that will keep vehicles or persons at least 80 feet away without being subject to controls. ▪ Provide fencing on the demarcation line at least 8 feet in height, from outside grade, with intrusion monitoring on the fence/wall. ▪ Ballistic wall should be considered if design includes an outside generator or other power facility.
Gates	P	▪ Provide for two entry/egress points. The secondary gate may be limited to emergency use only. ▪ Hydraulic rolling gates controlled by card access are recommended. ▪ All entry/egress points will have video surveillance. ▪ Intrusion alarm systems will be installed along gates. ▪ All gates will be provided with alarm contact points.
Interior Roadways	P	▪ Traffic calming in the form of traffic circles should be used if the interior roadways are of sufficient length ▪ Use of bollards near the building itself is essential
Lighting		▪ Provide visible light in the parking areas. ▪ Provide visible light or infra light in all other exterior areas to allow CCTV surveillance
Landscaping: Crime Prevention Through Environmental Design (CPTED)	P	▪ Vegetation will be designed to eliminate areas providing concealment from CCTV and roving patrol guards. ▪ Boulders, berms, or other impediments will be designed protecting all buildings from vehicle attack.
Signage	P	▪ Signs will be provided to identify trespassing, video surveillance, and/or firearms regulations based on IROC/local standards.
Doors		▪ More secure areas require higher security doors. Exterior doors and doors to identified high-risk areas are to be the strongest. ▪ Astragals should be used on perimeter doors ▪ Security hinges, with non-removable pins, on all controlled doors. ▪ All locks are high security cylinders on a master keyed system controlled by IROC

Design Feature	Type	Design Recommendation
Access Control System (ACS)		▪ Utilize an automated card access control system to provide control at gates, perimeter entry points, and different areas of the building, based on design and use of the area. ▪ Use the system to separate public areas from all other areas. ▪ Use the system to further segregate higher security areas within the facility.
Intrusion Detection System (IDS)	P	▪ The entire perimeter will be alarmed with appropriate technology for the type of fence. ▪ Perimeter entry points to the buildings (doors, windows, hatches) will be alarmed ▪ Intrusion alarms will be installed at critical areas, as necessary. ▪ All intrusion detection devices will be hardwired to the ACS or DVMS with detection and tamper alarming capabilities. ▪ All gates to be alarmed
Closed-Circuit Television (CCTV) and Digital Video Management System (DVMS)	P	▪ Fixed and PTZ cameras will be installed to view the entire perimeter from multiple angles. ▪ Interior CCTV will be utilized at critical areas for both security and safety purposes (e.g. reception area) ▪ All cameras will be capable of both “touring” and alarm assessment. ▪ A networked digital video management system will provide simultaneous live view/recorded view/playback/record across the network. ▪ Multiple workstations can be provided, if required. ▪ Video motion alarming will be used as secondary detection on the perimeter. ▪ CCTV will have full integration with IDS and ACS. ▪ The system will be scalable to the Enterprise level. ▪ The system will be capable of distributing the video by multiple technologies ▪ The video will be watermarked or otherwise protected for evidentiary purposes

Design Feature	Type	Design Recommendation
Systems Integration and Networking	P	▪ IDS, ACS, CCTV and DVMS systems will be fully integrated via an intelligent software interface. ▪ IDS or ACS breaches will call CCTV and DVMS systems to the breach for secondary alarm verification, assessment, and response. ▪ There will be the capability to "see" all the systems from one workstation – local or remote. ▪ All security systems within the facility will run over a dedicated security network.
Electrical System	P	▪ All security systems will have local battery back-up with a minimum battery back-up time of four hours ▪ The security systems will also be connected to UPS backup and/or generator backup sources for long-term outages.
System Monitoring	P/A	▪ On-site monitoring will provided for guards. ▪ The system will have the capability to add monitoring points, both local and remote, as necessary in the future.
System Maintenance	A	▪ The project specification should provide operational support requirements that include a preventative maintenance program and emergency service/repair response times.
Systems Training	A/P	▪ System specifications to include training requirements for operators, administrators, and maintenance of the integrated security systems
Security Policy	A	▪ The security program for this facility requires security policy development specific to the needs and operational character of this site. The existence of multiple agencies within the facility means that no one agencies existing policy will suffice.
Security Procedures	A	▪ It is recommended that IROC develop Standard Operating Procedures for security procedures and system preventive maintenance/calibration, addressing the following issues: – Facility access measures for visitors and contractors; – Photo identification badging – Lock up procedures; – Key control procedures; – Deprovisioning; – Records management; – Incident reporting; and – Preventative maintenance program

Design Feature	Type	Design Recommendation
Security Awareness Training	A	▪ It is recommended that the IROC develop a security awareness training program to deliver to persons working at the facility.
System Performance Measurement	A	▪ It is recommended that IROC select an agency or organization to conduct inspection and testing services periodically, and security system performance tests. ▪ It is recommended that IROC security staff perform periodic security procedures tests.
Security Continuity of Operations	A	▪ IROC to develop a Business Continuity Plan specific to this facility and operation