



**PROPOSAL FOR SECURITY
ASSESSMENT & DESIGN SERVICES
FOR THE IOWA DEPARTMENT OF
ADMINISTRATIVE SERVICES
RFB0920005016**

APRIL 30, 2020



Prepared for:





EXHIBIT 1 - TRANSMITTAL LETTER





April 29, 2020

State of Iowa Department of Administrative Services
Attn: Randy Worstell
Hoover State Office Building, Level 3
1305 East Walnut Street
Des Moines, IA 50319-0105

RE: RFB0920005016 – Security Assessment and Design Services

Dear Mr. Worstell,

The State of Iowa is looking to engage with a consultant to provide security assessments and designs on a wide range of buildings and properties for state and local agencies, including office buildings and government facilities. When undertaking these kinds of projects, the goal is to increase safety and security for the employees and users of the facilities by understanding the overall risks and vulnerabilities for each facility/site, recommending options for improvements that eliminate or mitigate those risks, producing security risk assessment reports and master plans, and providing schematic design for physical improvements, where necessary.

iParametrics is dedicated to creating solutions for our clients that increase safety, minimize vulnerabilities, and allow them to operate with peace of mind. We have been in business since 2003, doing this work for clients across the country, including on demand services contracts much like this one in New Mexico. Our goal is the same as yours: **To provide an accurate, efficient, and thorough security assessment to inventory, identify, and update the security in facilities and provide a safe place for staff and the public to do business.** Our experience and knowledge of best practices means that we can bring a wide range of solution options to bear for the state.

Your evaluation criteria emphasized the desire to select a contractor with highly qualified, skilled, and trained professionals with:

- **The experience and reputation in executing similar projects.** We have performed similar tasks for state and local agencies across the United States, including active projects with the states of Washington, New Mexico, Florida, Kentucky, and Vermont. This experience means that iParametrics is exceptionally well-qualified to assist the state in the assessment of your facilities. We have an in-depth knowledge of the threats and risk elements common to government facilities. Our staff has performed over 7,000 physical security risk assessments in support of local, state, and federal agencies throughout the United States, including municipal facilities from city halls to urban government complexes, from local cities and counties to the U.S. Capitol Complex in Washington, DC.
- **The technical abilities and solutions to not only meet deliverables but exceed expectations.** Having assessed thousands of federal, state, and local facilities throughout the country, our staff understands the complex nature of this assignment, not just from a compliance standpoint but also from an operational one. We have developed an approach that takes into consideration your needs for high quality services, timely deliverables, and the stated goals within the scope of work. We understand the critical importance of issuing all of the plans and deliverables within your required deadlines and within budget. We have developed our approach to ensure that we fulfill our contractual obligations and issue the stated deliverables in a timely manner. **Our goal is to always meet or exceed your expectations; it is what has made us successful throughout our 16 years in business.**
- **A notable track record providing clients a timely, cost-effective, and valuable engagement.** We know quality people drive quality results, which is why our commitment to you starts with the hand-picked engagement team we will assign to this project. Our Project Manager, Eddie Wise, has over 35

years of hands-on experience supervising emergency management, security, and law enforcement operations and forces around the world. He manages all of iParametrics' critical infrastructure assessment programs and is a nationally recognized subject matter expert on security planning, risk assessment, and mitigation. He leads a risk management, resilience, and mitigation team with significant experience performing federal, state, and municipal security assessments. **He has not only a notable, but a lengthy, track record of providing clients with timely, cost-effective, and valuable services in his areas of expertise**

As you will see throughout our attached proposal, iParametrics excels in all of these areas. Our response reflects an experienced technical team with the resources, proven methodology, experience, and commitment to provide optimum service and add value to the State of Iowa. **For these reasons and more, we believe iParametrics is the right choice for this program.**

As a principal of iParametrics, I offer my personal commitment to providing the State with the best resources and services available. If you need to contact me at any time, either before or after your selection decision, please call me at 678.381.2322 or email at paul.pelletier@iparametrics.com with any additional questions. All proposal terms, including price, will remain firm for a minimum of 120 days from the submittal deadline.

Sincerely,

A handwritten signature in black ink, appearing to read "P.S. Pelletier, Jr.", with a stylized flourish at the end.

Paul S. Pelletier, Jr.

Principal

iParametrics, LLC



EXHIBIT 2- EXECUTIVE SUMMARY





EXHIBIT 2

EXECUTIVE SUMMARY

We have read the full Request for Proposal and understand/agree to all of the terms and conditions, including the Contract Provisions in Section 6.

WHO IS IPARAMETRICS?

Founded in 2003 and headquartered in Atlanta, Georgia, iParametrics, LLC, is a recognized leader in security assessment and design for federal, state, and local agencies. We have supported clients in all 50 states, including projects throughout the state of Iowa.

iParametrics has over 100 employees, including certified security and risk professionals (CPP, PSP, CSC, ICS) and licensed professional engineers (PE).

Our experience includes working with over a dozen federal agencies and 300+ cities, counties, townships, and parishes throughout the United States. This includes recent work with the states of **Washington, New Mexico, and Vermont**; the counties of Arlington and Chesterfield, Virginia; the counties of Mecklenburg and Johnston, North Carolina, and the county of Larimer, CO to conduct facility security assessments and develop their physical security programs to protect their facilities, employees, and customers.

Recently we have been working for the Western Area Power Administration, and the US Army at their facilities located throughout Iowa conducting security assessments and developing detailed plans for upgrades to the physical and electronic security systems supporting protection of their critical infrastructure.

iParametrics is not affiliated with any security technology manufacturer or product. We do not install or maintain electronic security systems. We do not provide armed or unarmed contract security services. **We are a truly independent consultant.**

UNPARALLELED FIRM AND STAFF EXPERIENCE, INCLUDING REFERENCES AT THE LOCAL, STATE, AND FEDERAL LEVEL

We have conducted security assessments and developed security plans and designs for countless clients throughout the nation. We understand the complexities associated with implementation of a security program and will take care to:

1. Provide complete confidentiality throughout the process; and
2. Ensure recommendations are realistic, cost-effective, and beneficial to the Client.

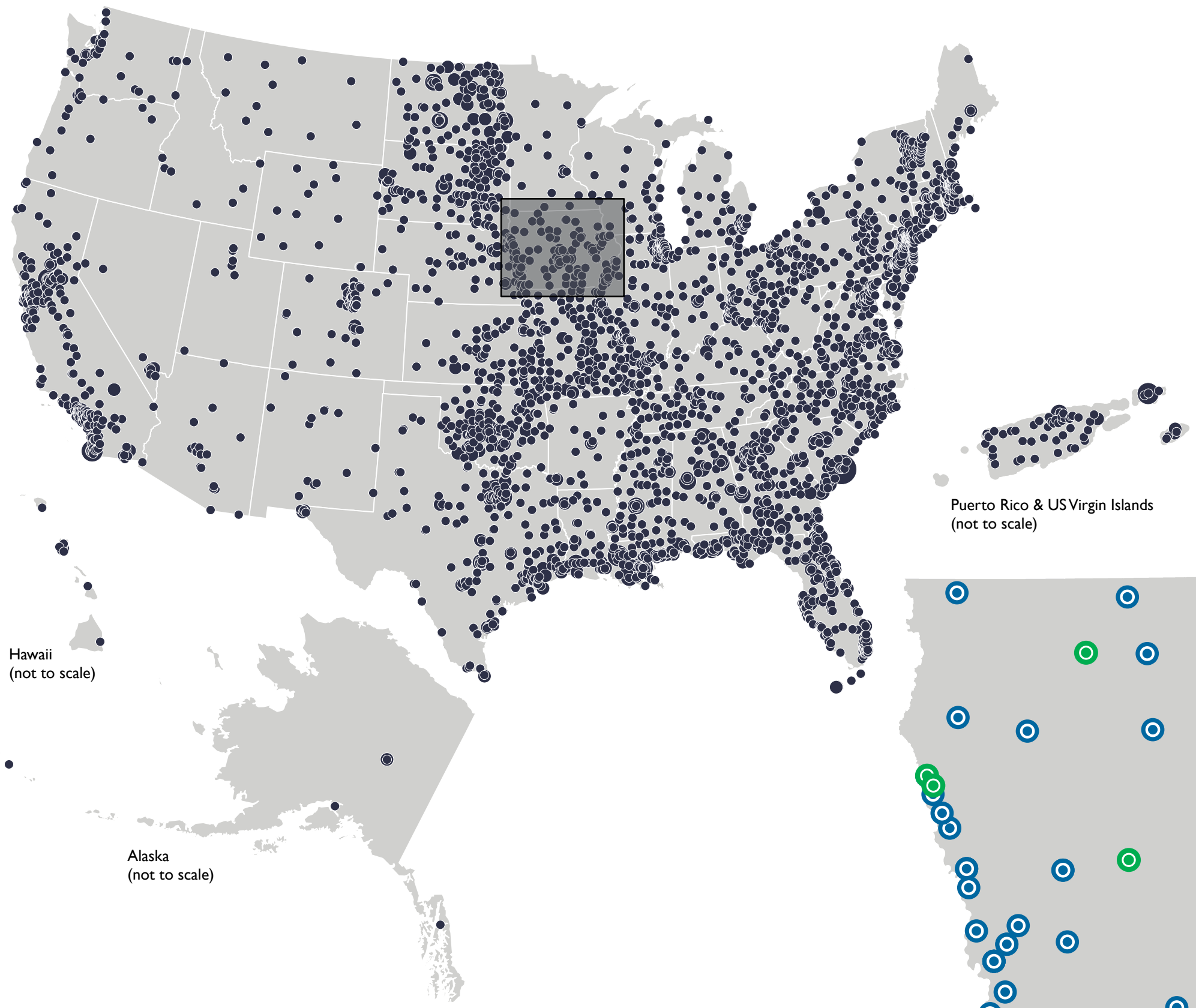
Our project lead, **EDDIE WISE, CPP**, Vice President of Security and Risk Management, has completed over 5,000 Physical Security Risk Assessments and maintains several active security clearances. Eddie has led similar engagements for the past 35 years and is considered a subject matter expert in this field.

With the fusion of qualified staff, unmatched experience, and proven methodology, our team is uniquely qualified to support the State.



EDDIE WISE, CPP
Vice President, Homeland Security





Hawaii
(not to scale)

Alaska
(not to scale)

Puerto Rico & US Virgin Islands
(not to scale)



Domestic Expertise
Proven past performance in all 50 states

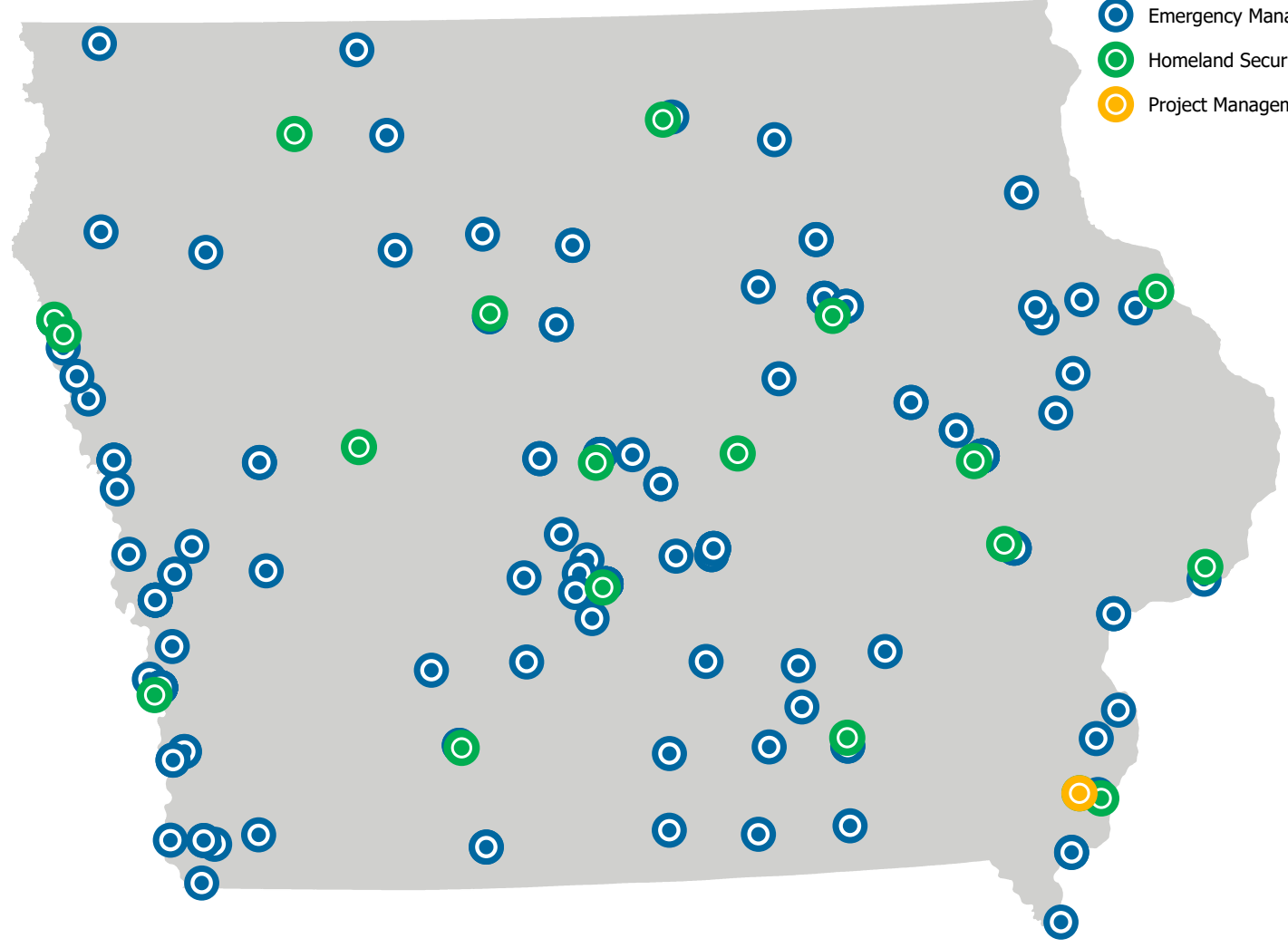


Customer Satisfaction
Dun & Bradstreet Open Ratings Score of 94



Past Performance
Performed over 7,000 security and all-hazard assessments for government facilities

- Emergency Management
- Homeland Security
- Project Management and Cost Engineering



PROVEN PROJECT APPROACH, CUSTOM TAILORED TO MEET THE NEEDS OF THE STATE OF IOWA

The iParametrics team understands the States objectives and the work requirements of this program. We will work in tandem with the State to provide project management for its execution and will utilize the lessons learned from our prior experience of administering multi-year, statewide security programs to ensure its successful delivery.

We are committed to delivering the highest quality product exceeding all customer expectations. On the next page, we have summarized the objectives outlined in the proposal and our ability to meet them.

TASK 1 - SECURITY ASSESSMENTS

Our security and risk professionals have worked with the Department of Homeland Security (DHS) Interagency Security Committee (ISC) and their Risk Management Methodology since the inception of the agency. We have refined their established process to fit a model more conducive to the operations and threats facing municipal governments. Our risk assessment process has been successfully implemented on hundreds of state, county, and city facilities across the nation.

Our risk process incorporates the best of the ISC Risk Management Process Tool while clearly recognizing the distinct differences between federal and municipal government facilities. Our process takes the ISC program a step further. Rather than just stopping at a risk score and identifying vulnerabilities, we develop a detailed Risk Register with multiple mitigation strategies, rough order of magnitude cost estimates, and an implementation plan. Each risk/vulnerability identified will be married with at least one solution/recommendation. Each recommendation will be actionable and realistic and may be related to processes, technology, or physical infrastructure.

TASK 2 - SECURITY DESIGN

We have extensive experience supporting projects for physical and electronic security system evaluation and design, including devices, technologies, and specialist materials for perimeter, external, and internal protection and response. This includes everything from security cameras, intrusion detection sensors, and closed-circuit television, to barriers, lighting, and access control. Our experience includes assessing, designing, estimating cost, and managing complex projects dealing with:

- Security cameras
- Access control systems
- Video surveillance and archiving systems
- Badging and credentialing systems
- Communications and response systems
- Security infrastructure such as fencing and barriers, fiber optic cable systems, electronic asset protection systems, and operations centers

The credibility of any security design program is a function of the competence of its manager and the security engineers. Our team is comprised of members of our highly trained technical staff with extensive experience in security and critical protection programs.

All staff members have extensive experience working with a variety of government



facilities and developing integrated and modern security solutions. We are independent and not affiliated with any security goods manufacturer, distributor, reseller, or representative.

WHY CHOOSE IPARAMETRICS?

iParametrics is exceptionally qualified to exceed your objectives as defined in paragraph 1.4 of the RFP. Our team of physical security professionals includes Department of Defense (DOD)-trained system designers who will be engaged to develop security schematics that will include current measures in place and proposed recommendations, where appropriate (e.g., fencing, bollards, guard booths, electronic arms, signage, truck checkpoint facility, etc.).

In addition, our security and risk management personnel have all been selected because of their past experience working at every level of government and private industry. We understand the unique requirement of public-facing state and local agencies and how to apply the necessary standards. We have a rigorous continuing education program that keeps our professionals abreast of the latest policies, procedures, technologies, and intelligence/threat breakthroughs.

QUALITY

We foster a culture of continuous improvement through our quality program and the regular analysis and reporting of performance measurement data to improve processes, procedures, and client services. We use independent client audits performed by Dun and Bradstreet to assess our performance and maintain a D&B Open Ratings Score of 94, which places our company in the top 10th percentile of firms in the United States. Our most recent audit report can be provided upon request and can be found on our [website](#).





EXHIBIT 3- FIRM PROPOSAL TERMS





EXHIBIT 3

FIRM PROPOSAL TERMS

The services being offered by iParametrics in this proposal are currently available. All proposal terms, including price, will remain firm for 120 days, as indicated on the cover sheet for the RFP.



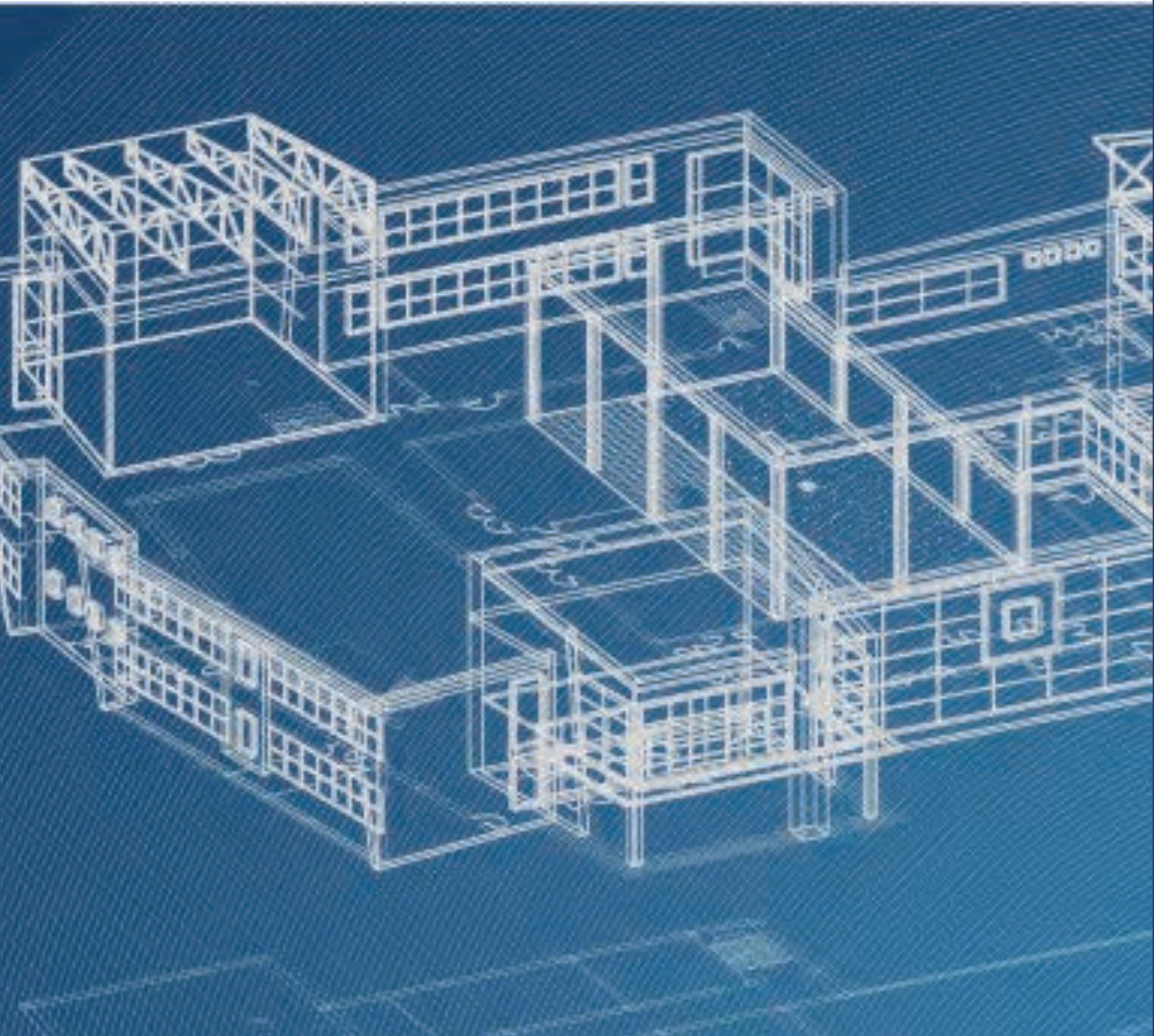


EXHIBIT 4- RESPONDENT BACKGROUND INFORMATION





EXHIBIT 4

RESPONDENT BACKGROUND INFORMATION

IPARAMETRICS

Founded in 2003, iParametrics is a recognized leader in homeland security and emergency management consulting. Headquartered near Atlanta, Georgia, with offices in New Jersey and North Carolina, we deliver a diverse range of emergency management and homeland security consulting services to a broad range of federal, state, and municipal clients throughout the country.



- **Does your state have a preference for in-state contractors?** Yes, although we are headquartered in Georgia, our clientele and approach to solutions has given us a strong cadre of security and engineering professionals across the country. For each Task Order issued under this contract we will identify the personnel best qualified to accomplish the task, the most cost-effective method of delivering the service to the client and what resources are available locally. Very often we discover that we already have personnel and/or partnerships in the community where we will be working. Whenever possible, we will employ those local resources to control costs without impacting performance.
- **Name, address, phone number, fax number, and email for the respondent**
iParametrics, LLC
178 South Main Street, Suite 100
Alpharetta, GA 30009
Phone: 770.664.6636
Fax: 770.664.6696
Email: eddie.wise@iParametrics.com
- **Form of business entity:** LLC
- **Copy of W-9:** Enclosed at the end of this section
- **State of incorporation, state of formation, or state of organization:** Georgia
- **Location (including addresses and phone numbers) of the offices or other facilities that relate to the Respondent's performance:**
iParametrics Security & Risk Management Project Office
1700 Pennsylvania Avenue, Suite 204, McDonough, Georgia 30253
Phone: 770.290.1470
- **Number of employees:** 78
- **Type of business:** Consulting firm
- **Name, address, and phone number of the representative to contact regarding all contractual and technical matters concerning the proposal:**
Paul Pelletier
178 South Main Street, Suite 100
Alpharetta, GA 30009
Phone: 770.664.6636
- **Name, contact info, and qualifications of any subcontractors who will be involved:** n/a
- **Respondent's accounting firm:** Windham Brannan, 3630 Peachtree Rd, NE, #600, Atlanta, GA 30326





EXHIBIT 5 - EXPERIENCE





EXHIBIT 5 EXPERIENCE

NUMBER OF YEARS IN BUSINESS

iParametrics has been in business for over 17 years, since 2003.

NUMBER OF YEARS OF EXPERIENCE WITH PROVIDING THE TYPES OF SERVICES SOUGHT BY THE RFP

Since 2005, iParametrics has continuously supported Homeland Security and Emergency Management operations throughout the United States. We have assessed risks and supported strengthening the infrastructure of numerous states and over 300 cities, counties, townships, and parishes throughout the country. This experience covers the entire spectrum of planning and mitigation including physical security and all-hazard risk assessments, plan and policy development, and security system design and testing.



Experience includes:

- Continuously supported Federal, State, and Local risk and mitigation programs since 2005
- Continually supported National Critical Infrastructure Protection Programs since 2010



THE LEVEL OF TECHNICAL EXPERIENCE IN PROVIDING THE TYPES OF SERVICES SOUGHT BY THE RFP

Our experience includes:

- **DEVELOPING ASSESSMENT STANDARDS AND PROGRAMS** to identify verifiable threats to facilities and evaluate existing countermeasures for the protection of employees, citizens, and facilities.
- **DESIGNING SYSTEMS AND MITIGATION STRATEGIES**, including producing engineering drawings and technical specifications prepared for procurement actions.
- **PROVIDING INFORMATION, RESEARCH, AND DATA RESOURCES** to support our decisions and recommendations.
- **CREATING WORKING RELATIONSHIPS** with our clients to build trust.
- **PROVIDING TRAINING SUPPORT** to develop, deliver, and evaluate training programs and courses based on these plans.

We work hand-in-hand with our clients to ensure their success. Our team is consistently on the cutting-edge of technology and works with our clients to apply various strategies to save time and money while enhancing security effectiveness, agility, and resilience.

Our project manager will be Eddie Wise, CPP, who has over 30 years of experience in security consulting.

A LIST OF ALL GOODS AND/OR SERVICES SIMILAR TO THOSE SOUGHT BY THIS RFP THAT THE RESPONDENT HAS PROVIDED TO OTHER BUSINESSES OR GOVERNMENTAL ENTITIES

- **Physical Security and All-hazard Risk Assessment.** We have performed almost 7,000 risk assessments for clients throughout the world. We emphasize the importance of developing critical relationships, preparing strategies and policies, and setting priorities. We offer practical guidance for planning effectively, spending wisely, and making communities safer. To assist in mitigating consequences from hazard events, we identify practical steps that agencies can take to be better prepared for all emergencies. Our recommendations support the industry's commitment to prevent those events that can be prevented and to minimize the impact of those that cannot.
- **Analytics and Modeling.** We can leverage a range of proprietary and commercial technology platforms, such as analytics engines and GIS modeling tools, to drive insight discovery of State operations, risks, and threats through data visualization. These tools have proven very effective at conveying risks to senior leaders and elected officials.
- **Plan and Policy Development and Evaluation.** We have extensive experience in developing and reviewing security and emergency plans, policies, and procedures. We can support the State to develop any necessary standards to enhance your overall security.
- **Security System Design and Testing.** Although we do not represent any manufacturer or endorse any product or technology, our employees have extensive technology experience related to facility security systems and security management. Our employees engage in the design, specification, evaluation,



testing, and supervision of a wide variety of state-of-the-art security systems on a routine basis and can provide integrated technical security solutions for client facilities. This work involves engineering, design, technical oversight, developing Statements of Work (SOWs), and project development.

- **Value Engineering Studies.** We have participated in over 30 value engineering studies and are well versed in the SAVE universally accepted VE Job Plan and Function Analysis System Technique (FAST). Our team members have significant experience in developing and analyzing cost-to-worth, cost-to-function, and cost-to-value relationships. We help establish and determine the needs of a facility, functional elements and systems, their associated functions, costs, and possible alternatives with the study team. We provide Pareto analysis of major cost drivers of a project, develop cost to benefit analysis of alternates, and are qualified to evaluate function, performance, worth, and cost of project elements. Our technique is directed toward analyzing the functions of an item or process to determine “best value,” or the best relationship between function, time, risk, and cost.
- **Program and Project Management.** We help our clients with successful project delivery through PMI-based management and technical principles, industry best practices, and the philosophy of quantifiable measurement of cost, schedule, technical performance, and quality management. In addition, we have technical staff and construction managers with decades of experience in the safe installation of electronic security systems who are available to assist the State to provide on-site supervision of the project.
- **Commissioning and Project Closeout.** Our technical team has extensive experience in the operation of a wide variety of electronic security systems and can assist Project Coordinators in putting a new system through its paces and identifying potential installation and operations issues prior to acceptance. We have experience performing field inspection, preparing and furnishing “as-built” drawings, and all facets of project closeout.
- **Preventative Maintenance (PM) and Testing Plans and Standards.** We have the ability to develop a preventative maintenance and testing plans for all equipment/systems in the client inventory per site. This would consist of clear and concise instructions and detailed procedures to be followed by technicians performing PM and testing of your systems. The plan will include testing the operations and performance of included system. This type of planning has been shown to extend the life of system components.
- **Training.** We have the ability to provide training to State personnel and contractors to perform all necessary administrative and operational functions of a system. We maintain our own Learning Management System (LMS) and can develop and host on-site and on-line learning courses for the State, as needed.
- **Source Selection and Procurement Support.** Our technical experts are experienced in the evaluation of contractor submissions and the intricacies surrounding procurement guidelines and regulations. We are prepared to develop bid documents and to provide the technical knowledge needed to evaluate proposal submissions for compliance with the SOW.
- **Integrity Monitoring/Anti-Fraud Services.** With two Certified Fraud Examiners (CFE) on staff, we have experience performing project audits, integrity monitoring, and fraud investigations on behalf of our clients.



LETTERS OF REFERENCE

Please see our attached letters of reference from:

- **Mecklenburg County** for our work on security assessment and enterprise risk planning for the County. Contact is **Mark Hahn**, Director of Asset and Facility Management, who can be reached at (980) 314-2520 or Mark.Hahn@MecklenburgCountyNC.gov.
- **Washington State** for our work on their security assessment and master plan for the Capitol Complex. Contact is **Bob Covington**, Director Capitol Security & Visitor Services, who can be reached at (360) 902-3570 or Bob.Covington@des.wa.gov.
- **Fluor Corporation** for our work on the FEMA Public Assistance contract. Contact is **Eileen McLaughlin** who can be reached at (703) 387-4826 or Eileen.McLaughlin@Fluor.com.





MECKLENBURG COUNTY Asset and Facility Management

LETTER OF RECOMMENDATION FOR IPARAMETRICS

From: Chad W. Harris, Security Director, Mecklenburg County Government

In 2017, Mecklenburg County advertised a Request for Qualifications to hire a security expert to develop a Security Master Plan for the County. After reviewing over 15 proposals, we determined that iParametrics demonstrated the best understanding of the County's needs and offered the best approach to achieve success. Upon award, iParametrics devoted the necessary resources and expertise to begin the project immediately. During the process, they listened and responded to the County's needs. They ultimately produced final reports that were comprehensive, sensible, and backed up by best practice data from across the country. Their wealth of resources, network, and ability to benchmark with similar sized local governments around the country is exceptional.

Within the Security Master Plan, iParametrics provided a summary about Crisis Management: recommended minimum structure for a Crisis Management Team (CMT), as well as noting resources, tools, etc. needed to operate an effective CMT. Based on my experience with updating and exercising a crisis management plan and CMT with a private sector company that had staff operating around the globe, including in high threat environments, their summary/vision for a crisis management program appears on point.

I would highly recommend iParametrics for Security Master Planning and Crisis Management Plan consulting.

A handwritten signature in black ink, appearing to read "Chad W. Harris".

Chad W. Harris, CPP
Security Director
Mecklenburg County Government

PEOPLE – PRIDE – PROGRESS – PARTNERSHIPS

3205 Freedom Drive, Ste. 101 Charlotte, North Carolina 28208 Phone (704) 432-0270 Fax (704) 432-0633

www.MecklenburgCountyNC.gov



STATE OF WASHINGTON
DEPARTMENT OF ENTERPRISE SERVICES

1115 Washington Street SE, Olympia, WA 98501
PO Box 41004, Olympia, WA 98504-1004

April 27, 2020

LETTER OF RECOMMENDATION FOR IPARAMETRICS

Dear Paul,

In 2018, the State of Washington embarked on a security assessment of the 468-acre Capitol Campus to identify vulnerabilities, risk mitigation strategies, and creation of a ten-year plan for deployment of mitigation strategies. Our Capitol Complex covers 468 acres and included over 4.5 million square feet of facilities supporting 46 state agencies. We selected iParametrics for their extensive expertise in security work, and especially their team's qualifications and background in security and risk management.

Due to the overarching and complex nature of the project, it required input and collaboration from across the State and included numerous elected officials, agency executives, security, and law enforcement professionals. The team started with an interactive discussion of our expectations and needs and then followed through with regular engagement and collaboration in evaluation of the Capitol Campus.

Finally, they performed spatial analysis and GIS modeling of our assets overlaid with statistical analysis of hazard exposure, crime, terrorism and risk profiles for a broad range of regional and local hazard events. These analytics provided insights into our risks and vulnerabilities measured against existing security operations, procedures and systems. Their ability to bring in this level of technology and expertise went beyond our expectations and proved especially helpful to our decision-making.

The iParametrics team brought deep knowledge and subject matter expertise to accomplish our project, and did so in a fast paced and often intense environment. The iParametrics report has provided a clear framework to support executive and legislative branch decision making in support of a safe, secure, and resilient Capitol Campus.

Thank You and the iParametrics Team for your contribution to the Washington State Capitol. I am happy to recommend the iParametrics team for future projects.

Sincerely,

Bob Covington
Director of Capitol Security & Visitor Services
Department of Enterprise Services



Fluor Enterprises, Inc.
2300 Clarendon Boulevard
Suite 1110
Arlington, VA 22201
USA

April 9, 2019

RE: Letter of Recommendation for iParametrics

To Whom it May Concern,

iParametrics has performed as a sub-contractor to Fluor Corporation on the DHS/FEMA Public Assistance contract since 2005 providing wide ranging technical expertise to projects throughout the United States in support of nationwide emergency planning, recovery and risk mitigation. This includes the evaluation and protection of public critical infrastructure including State and local government buildings, judicial facilities, K-12 schools, colleges and universities, hospitals and lifeline utilities such as power and water systems. Under this contract, iParametrics has participated in FEMA's Multiple Government projects since 2006 and has supported hundreds of state and local entities throughout the country. They have supported all technical elements of this program including the technical evaluation of critical infrastructure systems, planning and grant development, public policy evaluation and review, risk and vulnerability, training, exercises and hazard mitigation.

The nature of this work is often times technically complex, unpredictable, highly scrutinized and time sensitive. Their team has performed in exceptional fashion, providing high quality work under often times stressful and exhaustive workloads for over 13 years. We have just successfully re-competed this program for another 5 years (5 years, \$600M) and look forward to their long-term participation and support of this program.

Please don't hesitate to contact me should you have questions.

Regards,

A handwritten signature in blue ink, appearing to read "Eileen McLaughlin", is positioned above the typed name.

Eileen McLaughlin
Fluor-FEMA PA Staffing Coordinator
703-387-4826 (o)
Eileen.McLaughlin@Fluor.com



EXHIBIT 6- TERMINATION, LITIGATION, AND DEBARMENT





EXHIBIT 6

TERMINATION, LITIGATION, AND DISBARMENT

In the past five years, iParametrics:

- HAS NOT had any contracts for our services terminated for any reason.
- HAS NOT had any damages or penalties assessed against or dispute resolution settlements entered into under any existing or past contracts.
- HAS NOT had any orders, judgments, or decrees of any Federal or State authority barring/suspending our right to engage in business, practice, or activity.
- HAS NOT had any litigation or threatened litigation, administrative or regulatory proceedings filed against the firm.
- HAS NOT had any irregularities discovered in any of the accounts maintained by the firm or on behalf of others.





EXHIBIT 7 - CRIMINAL HISTORY AND BACKGROUND INVESTIGATION





EXHIBIT 7

CRIMINAL HISTORY AND BACKGROUND INVESTIGATION

iParametrics hereby explicitly authorizes the Agency to conduct criminal history and/or other background investigation(s) of the Respondent, its officers, directors, shareholders, partners and managerial and supervisory personnel who will be involved in the performance of the Contract.

A handwritten signature in black ink, appearing to read "P. Pelletier", written over a horizontal line.

Signed by: Paul Pelletier, Principal





EXHIBIT 8- ACCEPTANCE OF TERMS AND CONDITIONS





EXHIBIT 8

ACCEPTANCE OF TERMS AND CONDITIONS

iParametrics acknowledges our acceptance of the terms and conditions of the RFP and the General Terms and Conditions without change.

A handwritten signature in black ink, appearing to read "P. Pelletier", written over a horizontal line.

Signed: Paul Pelletier, Principal





EXHIBIT 9- CERTIFICATION LETTER



**Attachment #1
Certification Letter**

(Date) 4/29/2020

Randy Worstell, Issuing Officer
Iowa Department of Administrative Services
Hoover State Office Building, Level 3
1305 East Walnut Street
Des Moines, IA 50319-0105

Re: RFP0920005016 - PROPOSAL CERTIFICATIONS

Dear Randy Worstell:

I certify that the contents of the Proposal submitted on behalf of **(Name of Respondent)** in response to **Iowa Department of Administrative Services** for RFP0920005016 for a Security Assessment & Design Services are true and accurate. I also certify that Respondent has not knowingly made any false statements in its Proposal.

Certification of Independence

I certify that I am a representative of Respondent expressly authorized to make the following certifications on behalf of Respondent. By submitting a Proposal in response to the RFP, I certify on behalf of the Respondent the following:

1. The Proposal has been developed independently, without consultation, communication or agreement with any employee or consultant to the Agency or with any person serving as a member of the evaluation committee.
2. The Proposal has been developed independently, without consultation, communication or agreement with any other Respondent or parties for the purpose of restricting competition.
3. Unless otherwise required by law, the information found in the Proposal has not been and will not be knowingly disclosed, directly or indirectly prior to Agency's issuance of the Notice of Intent to Award the contract.
4. No attempt has been made or will be made by Respondent to induce any other Respondent to submit or not to submit a Proposal for the purpose of restricting competition.
5. No relationship exists or will exist during the contract period between Respondent and the Agency or any other State agency that interferes with fair competition or constitutes a conflict of interest.

Certification Regarding Debarment

I certify that, to the best of my knowledge, neither Respondent nor any of its principals: (a) are presently or have been debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by a Federal Agency or State Agency; (b) have within a five year period preceding this Proposal been convicted of, or had a civil judgment rendered against them for commission of fraud, a criminal offense in connection with obtaining, attempting to obtain, or performing a public (federal, state, or local) transaction or contract under a public transaction, violation of antitrust statutes; commission of embezzlement, theft, forgery, falsification or destruction of records, making false statements, or receiving stolen property; (c) are presently indicted for or criminally or civilly charged by a government entity (federal, state, or local) with the commission of any of the offenses enumerated in (b) of this certification; and (d) have not within a three year period preceding this Proposal had one or more public transactions (federal, state, or local) terminated for cause.

This certification is a material representation of fact upon which the Agency has relied upon when this transaction was entered into. If it is later determined that Respondent knowingly rendered an erroneous certification, in addition to other remedies available, the Agency may pursue available remedies including suspension, debarment, or termination of the contract.

Certification Regarding Registration, Collection, and Remission of Sales and Use Tax

Pursuant to *Iowa Code sections 423.2(10) and 423.5(8) (2016)* a retailer in Iowa or a retailer maintaining a business in Iowa that enters into a contract with a state agency must register, collect, and remit Iowa sales tax and Iowa use tax levied under *Iowa Code chapter 423* on all sales of tangible personal property and enumerated services. The Act also requires Respondents to certify their compliance with sales tax registration, collection, and remission requirements and provides potential consequences if the certification is false or fraudulent.

By submitting a Proposal in response to the (RFP), the Respondent certifies the following: (check which box that is applicable).

- Respondent is registered with the Iowa Department of Revenue, collects, and remits Iowa sales and use taxes as required by *Iowa Code chapter 423*; or
- Respondent is not a “retailer” or a “retailer maintaining a place of business in this state” as those terms are defined in *Iowa Code subsections 423.1(47) and (48)(2016)*.

Respondent also acknowledges that the Agency may declare the Respondent’s Proposal or resulting contract void if the above certification is false. The Respondent also understands that fraudulent certification may result in the Agency or its representative filing for damages for breach of contract in addition to other remedies available to Agency.

Sincerely,



Signature

Paul S. Pelletier, Principal
Name and Title of Authorized Representative

4/29/2020
Date



EXHIBIT 10- AUTHORIZATION TO RELEASE INFORMATION



Attachment #2
Authorization to Release Information Letter

(Date) 4/29/2020

Randy Worstell, Issuing Officer
Iowa Department of Administrative Services
Hoover State Office Building, Level 3
1305 East Walnut Street
Des Moines, IA 50319-0105

Re: RFP0920005016- AUTHORIZATION TO RELEASE INFORMATION

Dear Randy Worstell:

iParametrics, LLC hereby authorizes the **Iowa Department of Administrative Services** ("Agency") or a member of the Evaluation Committee to obtain information regarding its performance on other contracts, agreements or other business arrangements, its business reputation, and any other matter pertinent to evaluation and the selection of a successful Respondent in response to RFP0920005016.

The Respondent acknowledges that it may not agree with the information and opinions given by such person or entity in response to a reference request. The Respondent acknowledges that the information and opinions given by such person or entity may hurt its chances to receive contract awards from the State or may otherwise hurt its reputation or operations. The Respondent is willing to take that risk.

The Respondent hereby releases, acquits and forever discharges the State of Iowa, the Agency, their officers, directors, employees and agents from any and all liability whatsoever, including all claims, demands and causes of action of every nature and kind affecting the undersigned that it may have or ever claim to have relating to information, data, opinions, and references obtained by the Agency or the Evaluation Committee in the evaluation and selection of a successful Respondent in response to the RFP.

The Respondent authorizes representatives of the Agency or the Evaluation Committee to contact any and all of the persons, entities, and references which are, directly or indirectly, listed, submitted, or referenced in the Respondent's Proposal submitted in response to RFP.

The Respondent further authorizes any and all persons, and entities to provide information, data, and opinions with regard to its performance under any contract, agreement, or other business arrangement, its ability to perform, business reputation, and any other matter pertinent to the evaluation of the Respondent's Proposal. The Respondent hereby releases, acquits and forever discharges any such person or entity and their officers, directors, employees and agents from any and all liability whatsoever, including all claims, demands and causes of action of every nature and kind affecting the Respondent that it may have or ever claim to have relating to information, data, opinions, and references supplied to the Agency or the Evaluation Committee in the evaluation and selection of a successful Respondent in response to RFP.

A photocopy or facsimile of this signed Authorization is as valid as an original.

Sincerely,



Signature

Paul S. Pelletier, Principal
Name and Title of Authorized Representative

4/29/2020
Date



EXHIBIT 11 - MANDATORY SPECIFICATIONS





EXHIBIT II

MANDATORY SPECIFICATIONS

iParametrics will comply with each specification in Section 4 of the RFP.

4.1 SECURITY ASSESSMENT REQUIREMENTS

4.1.1 Respondent must be certified by the American Society for Industrial Security as a Certified Protection Professional (CPP) or Physical Security Professional (PSP) or a Certified Security Consultant (CSC) or equivalent association.

YES. Our team is comprised of security experts who are active in ASIS International and are credentialed or certified by federal, state, and local agencies as security professionals. Their credentials include ASIS certifications of Certified Protection Professional (CPP) and Physical Security Professional (PSP); the ISC certification of Certified Information Systems Security Professional (CISSP); the ISACA's Certified Information Security Manager (CISM); and the Department of Homeland Security's Interagency Security Committee (DHS-ISC) certification. This includes our Project Manager Eddie Wise, who is a Certified Protection Professional (CPP).

4.1.2 Respondent must have the ability to perform security assessment of State of Iowa facilities and/or Subs.

YES. We have the staff to provide a timely, cost-effective, and valuable engagement. We know quality people drive quality results, which is why our commitment to you starts with the hand-picked team we will assign to this project. Our Project Manager, Eddie Wise, CPP, has over 35 years of hands-on experience leading physical security, emergency management, security engineering, and law enforcement operations and programs around the world.

Our team is composed of subject matter experts in security assessments and design, including risk managers, emergency planners, and threat analysts. Our team has performed risk and resiliency assessments for critical infrastructure and utilities throughout the country and has extensive experience working with agencies throughout the United States.

We have continuously supported DHS National Critical Infrastructure Protection Programs since 2010 and conducted over 7,000+ physical security and all-hazards assessments.

4.1.3 Respondent must have the ability to recommend solutions to eliminate/mitigate risk and safeguard employees, guests, general public, and State resources.

YES. With thousands of security assessments completed by our team for the past two decades, we have the ability and expertise to recommend solutions to eliminate / mitigate risk and safeguard employees, guests, general public, and state resources.



4.1.4 Respondent must have the ability to review current security systems (e.g. access control, intrusion detection, video surveillance and monitoring, lock and key control) and identify security related threats from internal and external sources for during and after operating hours.

YES. The principles of an effective physical security program are Deter, Detect, Assess, Delay, Respond, and Recover. We are often called upon by our clients to do an assessment or review of current security systems for effectiveness, performance, and their ability to support these principles. Using our experience and expertise allows us to identify mitigation strategies to ensure the optimal level of protection is achievable and to allow leadership to make informed, risk-based decisions.

4.1.5 Respondent must have the ability to identify and make recommended actions that mitigate and/or eliminate risk.

YES. Every assessment completed by our team includes a tiered implementation strategy. Based on the results of the risk assessment, we develop a series of mitigation recommendations. Each of the recommendations includes a rough order of magnitude cost estimate and an estimate of risk reduction to identify return on investment.

4.1.6 Respondent shall provide a report containing recommendations for number, type, description, specifications and location of assessment and provided suggested methods for correction and/or mitigation.

YES. Our Security Assessment reports will, at a minimum, include the following:

- a) The **Narrative Analysis** will address existing conditions and unauthorized access vulnerabilities to all facilities and perimeters associated with the facility.
- b) The **Threat Vector Analysis** will provide specific details about the characteristics of each event that might take place at the facility. This will include a threat vector analysis specific to the facility assessed and is based on a worst-reasonable-case scenario. Each event provides sufficient information from which the threat, consequences, and vulnerability can be estimated in the conduct of a risk assessment.
- c) **Facility Security Guidelines** and recommended Levels of Protection (LOP) for the facilities will be provided.
- d) **Benchmarking (Comparative assessment)** will be used to compare processes and performance metrics to industry best practices from other similarly sized agencies throughout the country. The recommendations will include detailed security specifications.
- e) **Findings** will be listed followed by **recommendations** and will specifically evaluate and discuss, but are not limited to:
 - a. Security department organizational design
 - b. Security staffing and deployment
 - c. The physical security technology that is being used, including the monitoring of cameras and recorded images
 - d. Security-related policies and procedures related to security incidents, including incident reporting and tracking
 - e. A review of the emergency alerting system and communications processes, including the radio dispatch system
 - f. Access management controls
 - g. Employee security orientation, crime prevention and security awareness/training programs



- f) **Cost Estimates and a Phased Plan** will be provided for physical renovations and improvement of existing conditions, including state-of-the-art security measures designed to protect employees and facilities. Additionally, grant/funding opportunities will be included.
- g) **Site Plan/Schematics** will be developed using the drawings and site plans provided. If an acceptable floor plan is not available, we will prepare one during the site assessment. We will show the current measures in place and proposed recommendations, where appropriate (e.g., fencing, bollards, guard booths, electronic arms, signage, truck checkpoint facility, etc.).
- h) An **Outlook Report** will be prepared. In many cases, the assessment-budgeting-implementation cycle (and the standards-development cycle) is lengthy and may exceed the value of current threat information. To support long-range planning and design-construction efforts, the outlook provides a description of what the threat's changes may be over time.
- i) **References** for supporting information and source reports are will be provided as applicable.
- j) **Photographs** will be provided with each final report.

4.1.7 Respondent shall furnish all labor, materials, equipment, and incidental items necessary to complete assessment.

YES. We can furnish all labor, materials, equipment, and incidental items necessary to complete this assessment.

4.1.8 Respondent employees may be subject to background check completed by the State of Iowa.

YES. We vet all of our team members before hiring. Most of them hold active public trust evaluations and/or federal security clearances. Our Project Manager holds a DOD Top Secret and a DOE Q clearances. We understand that our employees may be subject to state and local background checks and are prepared to fulfill any requirement.

4.1.9 Respondent shall respond to assessment request within 48 hours.

YES. Rapid response is part of our DNA. As a FEMA Public Assistance vendor, we are often called on to respond immediately to disaster areas. Our project management teams provide 24/7 monitoring of phone and email systems. Our team stands ready to begin work within 48 hours of a request.

4.1.10 Respondent must maintain the minimum insurance requirements stated in Section 6.3.3.

YES. Our current corporate insurance coverage meets or exceeds all requirements.

4.1.11 Respondent shall not be in the business of selling security systems hardware.

YES. We are independent and not affiliated with any security goods manufacturer, distributor, reseller, or representative.

4.1.12 Respondent shall adhere to work rules of the applicable facility.

YES. We understand the varied operations of state and local facilities based on mission, criticality, and public access. We will work closely with clients to ensure our performance respects all rules and guidelines for access, operations, and privacy.



4.2 SECURITY SYSTEM DESIGN REQUIREMENTS

4.2.1 Certified by the American Society for Industrial Security as a Certified Protection Professional (CPP) or Physical Security Professional (PSP) or a Certified Security Consultant (CSC) or equivalent association.

YES. As noted above, our team is comprised of ASIS-certified CPPs and PSPs, and DHS-ISC-certified personnel. This includes our Project Manager Eddie Wise, who is a Certified Protection Professional.

4.2.2 Respondent must have the ability to perform facility security system design for the State of Iowa facilities and/or subcontractors.

YES. We have extensive experience with physical and electronic security system evaluation and design. Our personnel have received extensive baseline and continuing education in a wide variety security systems and physical countermeasures. We are experienced with complex systems, including devices, technologies, and specialized materials for perimeter, external, and internal protection and response. This includes everything from security cameras, intrusion detection sensors, and closed-circuit television, to barriers, lighting, and access control.

4.2.3 Respondent must have the ability to design solutions to eliminate/mitigate risk and safeguard employees, guests, general public, and State resources.

YES. Our team understands the missions of government. We recognize the need for a balance between security, safety, and access to the public. Our mitigation strategies are specifically designed to protect employees, guests, and property while still allowing government to provide those essential services the community needs.

4.2.4 Respondent must have the ability to design security systems (e.g. access control, intrusion detection, video surveillance and monitoring, lock and key control) and recommend security related threats from report containing recommendations for number, type, description, specifications and location of assessment, and provided suggested methods for correction and/or mitigation.

YES. We have performed over 7,000 physical security and all-hazards risk plans and projects and are backed by ASIS-certified experts and Professional Engineers who have deep subject matter expertise in designing security systems and other systems. We have a staff of security specialists, engineers, and designers to build the solutions for this project, backed by decades of similar project experience and expertise.

4.2.5 Respondent shall furnish all labor, materials, equipment, and incidental items necessary to complete design.

YES. Our personnel are trained and equipped to accomplish every potential task required during a security assessment. They are issued the personal protective equipment and are provided with the specific OSHA-level safety skills needed to accomplish the mission. They have light meters, digital cameras, measuring devices, and access to a full array of additional tools to ensure a complete and accurate assessment. Our engineering personnel can produce design and construction level drawings in a variety of CAD formats. Our team of talented designers are skilled at working with engineers and architects to develop mitigation system solutions in a wide spectrum of circumstances.



4.2.6 Respondent employees may be subject to background check completed by the State of Iowa.

YES. We understand that our employees may be subject to background checks and are prepared to fulfill this requirement.

4.2.7 Respondent must maintain the minimum insurance requirements stated in Section 6.3.3.

YES. Our current corporate insurance coverage meets or exceeds all requirements.

4.2.8 Respondent shall not be in the business of selling security systems hardware.

YES. We are independent and not affiliated with any security goods manufacturer, distributor, reseller, or representative.

4.3 POST DELIVERY DOCUMENTATION

Respondent must provide the assessment reports and recommendation only to the requesting agency and copies cannot be release without written consent of that Agency or proper authority.

YES. We take confidentiality very seriously. We will provide assessment reports and recommendations ONLY to the requesting agency and no copies will be released without written consent of that Agency or proper authority.





EXHIBIT 12- SECURITY ASSESSMENT SERVICES





EXHIBIT 12

SECURITY ASSESSMENT SERVICES

DESCRIBE RESPONDENT'S EXPERIENCE IN PERFORMING SECURITY ASSESSMENTS AND TECHNICAL SECURITY DESIGNS FOR MUNICIPAL FACILITIES. DEMONSTRATE EXPERIENCE IN CONDUCTING SECURITY WORK FOR GOVERNMENT INSTITUTIONS OF SIMILAR OR LARGER SIZE AND SCOPE.

FACILITY EVALUATION AND ELECTRONIC SECURITY SYSTEMS DESIGN FOR LARIMER COUNTY, CO

Just outside of Denver, CO, the Ranch Events Complex is a 244-acre site located in Larimer County. The 375,000-square foot complex hosts over 2,000 events a year and includes the First National Bank Building, which has 36,000 square feet of exhibition space, the Budweiser Events and Athletics Complex, a 7,200 seat multi-purpose arena, and several other large public facilities that support conferences and trade shows, sporting events, outdoor festivals and concerts, and livestock shows.

Under this program, iParametrics conducted an in-depth evaluation of the existing security systems with special emphasis on the CCTV system. We developed a detailed solution for the phased procurement of a new facility-wide integrated CCTV system, including detailed design specifications and drawings. Final deliverables included a comprehensive statement of work, detailed design specifications and drawings, and a detailed cost estimate to aid in procurement.

All work was completed on time and within budget.

REFERENCE

Mark Tinklenberg, Senior Operations Manager
Phone: (970) 619-4016
Email: tinklenm@co.larimer.co.us

CHESTERFIELD COUNTY SECURITY CONSULTANT, CHESTERFIELD COUNTY, VIRGINIA

Chesterfield County is one of the metropolitan counties adjacent to Richmond, Virginia, the seat of the Virginia State Capital. The County supports a population of 350,000 people and is part of the tri-cities area which includes the three independent cities of Petersburg, Colonial Heights, and Hopewell. In 2019, iParametrics was awarded a five-year contract as the County's security consultant. The scope of work includes:

- **Providing Physical Security Assessments for County infrastructure.** This includes threat assessments, risk assessments, and vulnerability surveys and recommendations of mitigation treatments supported by conceptual design and cost estimates.
- **Participating in the design phase** (programming schematic, design development and construction document phase) of projects. This includes developing the



design intent of all building security systems and subsystems.

- **Assisting County staff in monitoring installation, testing, commissioning, and operation of all security systems.**
- **Assisting County Staff with security and emergency planning, analytics, training, and exercises.**
- **In coordination with County, designer/engineer, sub-contractors and installers, developing a concept of operation and preparing design documents and specifications for security systems.**

As part of this contract, we are currently performing physical security risk assessments on 42 county sites, including the government complex, law enforcement facilities, airport, libraries, schools, and other government facilities.

The project entails detailed evaluations of County facilities, staff, and plans with the goal of improving and enhancing the security and safety of employees and visitors in each County facility. The deliverables will include a complete report of assessment findings, recommendations for conceptual design of risk treatments, and rough order-of-magnitude cost estimates for budgeting purposes.

REFERENCE

Jason Stone, PSP, Security Manager
Phone: (804) 717-6779
Email: stoneja@chesterfield.gov

ARLINGTON COUNTY SECURITY ASSESSMENT SERVICES, ARLINGTON COUNTY, VIRGINIA

iParametrics was selected by Arlington County to support a 5-year security contract, which includes all-hazards assessment of County infrastructure. Arlington County, located in the Commonwealth of Virginia, is home to over 234,000 residents, making it the sixth largest county in the state.

In 2019, iParametrics was selected to work alongside the County's Security Working Group to perform a comprehensive security assessment, issue recommendations to mitigate risk, and develop an actionable and realistic implementation plan for the County owned and operated Bozman Government Center. Arlington County occupied space within 10 public mixed-use floors out of the 13-story building, which sat on a four-level parking garage open to private and public use. The scope of work for this project includes:

- Complete an assessment of critical infrastructure, ESS systems, operations (including guard force management and staffing models), polices, plans, procedures, and dependencies and from these develop a series of recommendations, plans, and mitigation strategies to minimize the risks to operations and disruption of services.
- Coordinate with the County's Project Manager to review the existing data resources (most recent Threat and Vulnerabilities Assessment, a list of all Critical Infrastructure Assets and facility information, security policies and procedures, electrical engineering files), and discuss project coordination and communication.

REFERENCE

Jeremy Jenkins
Phone: (703) 228-6526
Email: jjenkins@arlingtonva.us



SECURITY RISK ASSESSMENT AND MASTER PLAN, BROWNSVILLE, TX

iParametrics supported the Brownsville Public Utility Board in developing and executing its Security Master Plan and security risk assessments. The Commission provides electric, water, and wastewater services to a 133-mile area, which encompasses the City of Brownsville, TX along the southernmost tip of Texas, on the northern bank of the Rio Grande, directly north and across the border from Matamoros, Tamaulipas, Mexico.

iParametrics provided a comprehensive security risk assessment to evaluate and make recommendations regarding the existing physical security measures, current emergency response protocols, training initiatives, current security policies and procedures, current staffing of contracted security services, current security communications, and current security surveillance systems from which to then develop a master plan. We assessed over 20 facilities including water and wastewater treatment plants, water towers, a power plant, electric substations, wastewater lift stations, office buildings, and other utility facilities. Some of these facilities are located on the United States-Mexico border and subject to transnational crime which occurs in the border region.

iParametrics has been awarded subsequent planning work to develop agency wide policies for:

1. **Access Control, Visitor Management and Key Control.** This policy outlined the baseline standards for any personnel needing to access to any the Commission facility.
2. **Electronic Security Systems Management.** This policy developed the specific duties and responsibilities for the pro-procurement, installation, maintenance, and monitoring of all electronic security systems employed in the Commission facilities. These systems include access control, intrusion detection, closed circuit television, and duress.
3. **Incident Reporting.** This policy developed the process and assigned duties and responsibilities for reporting of specific incidents occurring on the Commission property or involving the Commission assets. Reporting formats, processes, actions, and timelines were defined.
4. **Guard Force Evaluation.** iParametrics developed the scope of work and acted as the City's technical reviewer of pro-posals for the City Guard Services Contract.

REFERENCE

Lucila Cano Hernandez, Director of Administrative Services

Phone: (956) 983-6280

Email: Lhernandez@brownsville-pub.com

ENTERPRISE SECURITY PLAN AND FACILITY ASSESSMENT, MECKLENBURG COUNTY, NORTH CAROLINA

In September 2016, a State of Emergency was declared for North Carolina and Mecklenburg County after historic riots and looting swept through the streets of Uptown Charlotte after the police shooting of Keith Lamont Scott on the afternoon of Sept. 20. As a result, iParametrics was retained by Mecklenburg County, NC to support the development of an enterprise security program and facility risk assessment to better help the city deal with the system shocks and stresses prevalent



within the rapidly growing and ethnically diverse metropolitan area. With a population of over 1.2M residents, Mecklenburg County is the largest county in North Carolina and home to the City of Charlotte.

The project entailed the development of an Enterprise Security Strategy and framework in support of over 120 county facilities (including parks and recreation facilities), 5,000 employees and 100 security officers. The first phase of work included the assessment of the county's security posture including the evaluation and development of the county's DBT, evaluation of county physical security systems, development of facility security levels (FSL) for county facilities, threat, vulnerability assessment, operational assessment, technology assessment, evaluation of the requirement for a Security Operations Center (SOC) and the development of a security master plan.

The project included the evaluation of a broad range of public infrastructure including municipal centers, court and judicial facilities, law enforcement and first responder facilities, detention centers, public parks, libraries, public parks, healthcare and clinical facilities, county maintenance facilities and leased office space. iParametrics was awarded a subsequent contract (\$189K) to further develop the counties security and crisis planning programs.

- Key structural elements of the program:
- Included 120 multi-tiered facilities (Level 1- Level 4)
- Broad and diverse range of municipal infrastructure supporting multiple agencies
- Aggressive completion schedule framed by the County budgeting cycle
- Due to the overarching and complex nature of the project, it required input and collaboration from across the organization and included elected officials.

As a result of the project, the County funded the development of a County Security Operation Center (SOC), improvements to security staffing and management systems, Electronic Security Systems (access control, intrusion, duress & CCTV) management and maintenance and incident reporting systems and improved procedures. iParametrics has been awarded a subsequent contract to further develop the county's security and crisis management programs. All work has been completed on time and within budget.

REFERENCE

Mark P. Hahn, AIA, Director of Asset and Facility Management

Phone: 980-314-2520

Email: Mark.Hahn@MecklenburgCountyNC.gov

STATE OF WASHINGTON PHYSICAL SECURITY PROGRAM, WASHINGTON

iParametrics was selected by the State of Washington to provide a comprehensive security review of the 468-acre Washington State Capital Campus. Our firm assessed over 4.5M square feet of facilities supporting 46 state agencies including the Governors Complex, State Senate, State Legislature, the State Supreme Court and the Attorney Generals Offices amongst others. The project also entailed the protection of Sylvester, Heritage, Marathon and Centennial parks, Capital Lake Park and Trails Complex, the Capital Lake Interpretive Center and Deschutes Parkway as well as memorials, monuments and art work on the campus grounds.

Working with the Washington State Patrol and a broad set of State stake-holders, we have:



- Assessed current capital campus security, to include infrastructure, physical security technology, organization, plans and resourcing of operations.
- Performed a comparative assessment of security systems and security operations of comparable state capital campuses.
- Identified opportunities to mitigate security vulnerabilities to support the safety and security of the capital campus.
- Developed a physical security risk assessment and phased plan for improving campus physical security and safety, to include conceptual security designs, estimated costs of individual recommendations and budgetary decision packages for those recommendations re-quiring funding during the 19/21 biennium.
- Performed spatial analysis and GIS modeling of client assets over-laid with statistical analysis of hazard exposure, crime, terrorism and risk profiles for a broad range of regional and local hazard events. Analytics provided keen insights into the states' risks and vulnerabilities measured against existing security operations and systems.

Key structural elements of the program:

- Large portfolio of State-owned facilities (approximately 4.5M square feet)
- Included multi-tiered facilities (Level 1-level 4)
- Broad and diverse range of public infrastructure including the State Capital buildings and facilities supporting 46 State agencies
- Aggressive completion schedule framed by the State budgeting cycle.
- Due to the overarching and complex nature of the project it re-quired input and collaboration from across the State and included the Lt. Governor, Senators, Congressmen and other State leader-ship.
- Multi-year program

In December 2018, the Governor's Operating Budget was published, which included numerous recommendations from the study. Funding for security improvements included organizational funding and the development of a State SOC, funding to update cameras, replace duress alarms in select buildings, the installation of a distributed antenna system (DAS) in campus garages, and to design and construct a utility redundancy line for emergency communications within the State Capital complex. All work has been completed on time and within budget.

While this is an ongoing project, all work was completed on time and within budget.

REFERENCE

Bob Covington, Director Capitol Security & Visitor Services

Phone: 360-902-3570

Email: bob.covington@des.wa.gov

PROVIDE AN ESTIMATE OF STATE OF IOWA STAFF TIME REQUIRED TO COMPLETE THE SECURITY ASSESSMENT.

The estimate for Iowa staff time is six to 12 hours per facility. This includes meetings, interviews, and escorts (when required).



DESCRIBE RECOMMENDED STRATEGY INCLUDING ON-SITE COORDINATION AND SUPPORT SERVICES, BEST PRACTICE CONSULTING OPTIONS AND PROFESSIONAL SERVICES.

iParametrics has supported numerous communities and agencies as they plan for and respond to threats and emergencies. We emphasize the importance of developing critical relationships, preparing strategies and policies, and setting priorities. We offer practical guidance for planning effectively, spending wisely, and making the nation's communities safer.

To assist in mitigating consequences from hazard events, we identify practical steps that our clients can take to be better prepared for all emergencies. Our recommendations support the industry's commitment to prevent those events that can be prevented and to minimize the impact of those that cannot. Emphasizing balanced, common-sense measures, we hope to assist the State through the evaluation of existing security systems and procedures for its facilities.

In coordination with your project team, we will define the processes, functions, activities, physical boundaries (facilities and locations), and stakeholders included within the boundaries of the projects. Within seven days of award, or upon a mutually agreed schedule, our Program Manager will meet with the Iowa project team for the initial project meeting to discuss project coordination and communication and to finalize the required data elements for the study.

Sound management and technical principles, industry best practices, and the philosophy of quantifiable measurement of cost, schedule, technical performance, and quality management will form the basis for project delivery to the State. Upon initiation of a project, we will prepare a cost estimate and a Microsoft Project schedule and maintain the schedule throughout and up to the closeout of the project. Our standard methodologies include arranging and conducting meetings as necessary and in conjunction with project milestones, which usually includes providing transcripts to participants within 72 hours.

We will provide the State with a comprehensive analysis and series of reports allowing appropriate managers to make risk-based decisions to prepare for and recover from a defined series of specific threat scenarios. Risk will be assessed using both a quantitative (parametric) approach and a qualitative (subjective) approach. Assessment conclusions will be based on verifiable evidence, where available, gathered through a systematic and proven risk assessment process that ensures reliability and reproducibility.

Furthermore, we will deliver a phased plan and recommendations for improving physical security and safety, which will include estimated costs of individual recommendations, draft budgetary decision packages for those recommendations, and an outlook report to support long-range planning and design-construction efforts. Additionally, the final documentation will include training recommendations and relevant grant/funding opportunities.

BASIC THREAT, VULNERABILITY AND RISK ASSESSMENT METHOD

Conducting an assessment of an organization requires knowledge of both internal and external factors that can influence the organization's performance in managing risks. The following elements will be considered throughout the project:

- a) The industry sector
- b) The organization's processes



- c) Internal factors affecting the organization's operating environment
- d) External factors affecting the organization's operating environment

Our process, which has been successfully implemented on several hundreds of municipal facilities, is in conformance with the ISC Risk Management Process for Federal Facilities, the DHS's Buildings and Infrastructure Protection Series (FEMA-426/BIPS-06) Reference Manual, and the Center for Development of Security Excellence's (CDSE) Risk Management methodology. This method closely approximates the ISO 31000-based Risk Assessment Standard RA. 1-2015, developed by the Risk and Insurance Management Society, Inc. (RIMS), American Society for Industrial Security (ASIS) International, and the American National Standards Institute (ANSI), [ANSI/ASIS/RIMS RA. 1-2015].

This methodology allows us to assess target value from the attacker perspective (essentially from the outside looking in) and from the client perspective (essentially inside looking out), as well as give asset owners a roadmap forward in mitigating and recovering from an undesirable event.

Understanding the key factors, drivers, and issues that influence an organization's ability to achieve its objectives and meet its obligations is an integral part of the planning process and will provide a foundation for assessment activities.

This method allows us to evaluate threats unique to the State and its agencies or hazards specific to a facility location, while standardizing how these threats and hazards are analyzed. This method yields quantitative measures of risk and compliance, enabling managers to make prioritized resource allocation decisions regarding the most effective mitigation options.

PROJECT EXECUTION

The risk identification process begins with an evaluation of current operations and critical infrastructure and their interdependencies. Asset characterization identifies what assets or facility elements may be at risk, what is their criticality to the organizational objectives/operations, and what are the potential consequences of those assets being compromised.

Our team will review the existing critical asset inventory provided by the State to clearly identify those facilities and systems necessary to maintain operations. This analysis will look at physical structures, specialized equipment, and automated systems necessary for the ordinary and crisis-related operations of the asset.

The team will also identify those ancillary assets that, while not under the State's control, provide integral support for uninterrupted service. For example, this could include other utility providers, fuel suppliers, transportation, and other supply chain-related operators.

The team will review in detail all of the physical protective measures (locks, windows, doors, ESS) and procedural measures (Physical Security Plan, Occupant Emergency



Plan, guard and security staffing and orders, etc.). During the hours of darkness, we will observe the facility to identify potential threats or hazards, such as poor lighting, illicit activity, or traffic issues.

RISK MEASUREMENT

Our risk measurement process begins by outlining the approach necessary to identify, assess, and prioritize the risks to the State's assets and operations. We then create a baseline Level of Protection (LOP) that mitigates vulnerabilities to threats and the potential consequences, thereby reducing risk to an acceptable level. The following process provides the method for determining the desired LOP of assets.

IDENTIFY ANY THIRD-PARTY RESPONDENTS INVOLVED IN RESPONDENT'S IMPLEMENTATION STRATEGY AND DESCRIBE THESE RELATIONSHIPS.

To ensure our drawings are completed in full compliance with all applicable local standards, any drawings requiring a stamp/signature will be routed through a professional engineer in the jurisdiction where the work is to be completed.

IDENTIFY THE TYPES OF DELIVERABLES THAT WOULD BE PROVIDED AS A PART OF THIS SERVICE.

The Security Assessment report will, at a minimum, include the following:

- a) A **Narrative Analysis** that will address existing conditions and unauthorized access vulnerabilities to all facilities and perimeters associated with the facility.
- b) A **Threat Vector Analysis** that will provide specific details about the characteristics of each event that might take place at the facility. This will include a threat vector analysis specific to the facility assessed and are based on a worst-reasonable-case scenario. Each event provides sufficient information from which the threat, consequences, and vulnerability can be estimated in the conduct of a risk assessment.
- c) **Facility Security Guidelines** and recommended Levels of Protection (LOP) for the State's facilities.
- d) **Benchmarking (Comparative assessment)** will be used to compare your processes and performance metrics to industry best practices from other similarly sized systems throughout the country. The recommendations will include detailed security specifications.
- e) **Findings and Recommendations** will be listed followed by recommendations and shall specifically evaluate and discuss, but are not limited to:
 - a. Security department organizational design
 - b. Security staffing and deployment
 - c. The physical security technology that is being used including the monitoring of cameras and recorded images
 - d. Security-related policies and procedures related to security incidents, including incident reporting and tracking
 - e. A review of the emergency alerting system and communications processes, including the radio dispatch system



- f. Access management controls
- g. Employee security orientation, crime prevention and security awareness/training programs
- f) **Cost Estimates and a Phased Plan** will be provided for physical renovations and improvement of existing conditions, including state-of-the-art security measures designed to protect client employees and facilities. Additionally, grant/funding opportunities will be included.
- g) **Site Plan/Schematics** will be developed using the drawings and site plans provided by the agency. If an acceptable floor plan is not available, we will prepare one during the site assessment. We will show the current measures in place and proposed recommendations, where appropriate (e.g., fencing, bollards, guard booths, electronic arms, signage, truck checkpoint facility, etc.).
- h) An **Outlook Report** will be prepared. In many cases, the assessment-budgeting-implementation cycle (and the standards-development cycle) is lengthy and may exceed the value of current threat information. In order to support long-range planning and design-construction efforts, an outlook section is provided to describe what is assessed to be the changes in the threat over time.
- i) **References** to supporting information and source reports are provided as applicable.
- j) **Photographs** will be provided with each final report.

For a Security design package, we will include an outline of system components and recommendations for installation. When required we can produce construction level drawings and a detailed statement of work for the procurement, installation, commissioning, training, and maintenance of all security systems.





EXHIBIT 13- SECURITY SYSTEM DESIGN SERVICES





EXHIBIT 13

SECURITY SYSTEM DESIGN SERVICES

DESCRIBE RESPONDENT EXPERIENCE WITH DESIGNING FACILITY SECURITY SYSTEMS AND SECURITY MANAGEMENT SYSTEMS

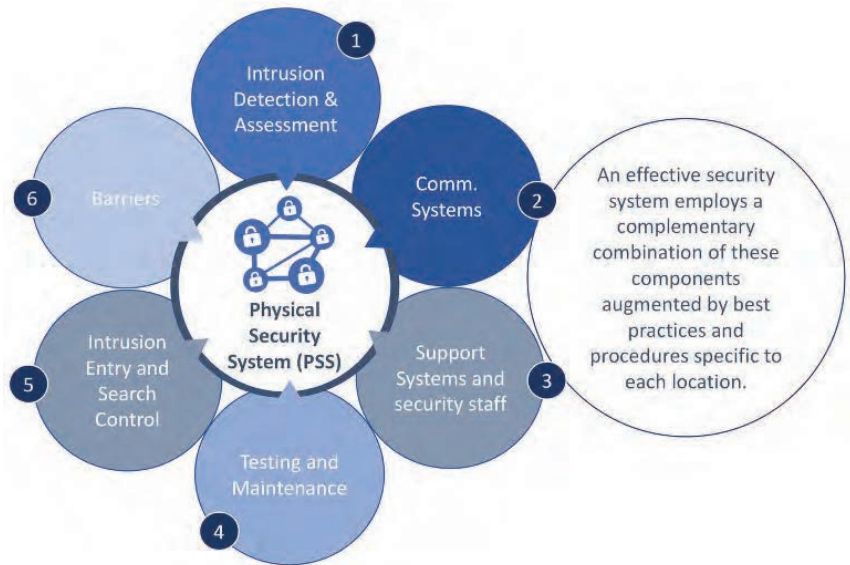
The time for using separate intrusion, CCTV, access control, duress, and other physical protective systems has passed. Systems now are designed to work as an integrated unit. Security should begin at the outermost perimeter of a facility and provide an ever-increasing concentric layers of security.

A physical protection system (PPS) integrates people, procedures, and equipment for the protection of assets or facilities against theft, sabotage, or other hostile human attacks. The design of an effective PPS requires a methodical approach in which the designer weighs the objectives of the PPS against available resources and then evaluates the proposed design to determine how well it meets the objectives. Our team of security professionals have designed systems for the protection of individuals facilities and large campuses. We have developed the design criteria, the statements of work, participated in source selection, provided oversight of installation, commissioning, and training.

As an example, iParametrics performed physical security assessments and developed risk-based security designs for Social Security Administration campuses throughout the country which includes significant locations throughout the State of Iowa. Our team assessed and analyzed existing security measures and practices in each facility, providing findings and recommendations for corrective action and developed conceptual designs and cost estimates to enhance SSA’s security program.

DESCRIBE RESPONDENT EXPERIENCE WITH DESIGNING ACCESS CONTROL, INTRUSION DETECTION, AND PERIMETER PROTECTION SYSTEMS.

As mentioned above, we have designed a wide variety of electronic security solutions. Our PSP professionals have been trained at the Army Corps of



Engineers electronic security systems engineering and design course. They have also provided instructor support for the same school. They attend continuing education training with multiple manufacturers to understand not only the capabilities of a system but the inner working, maintenance, and troubleshooting requirements.

We do not limit ourselves to a single solution, but focus on solutions that fit a client organization. For example, we recently worked with a customer who had installed a very sophisticated and robust enterprise security program. However, they were only using the system for their access control, essentially making it a replacement for the key control system. We worked with them to integrate their existing cameras, intrusion detection, and duress systems into the platform. We are guiding them in the next steps of incorporating law enforcement response and emergency notification into the same system.

DESCRIBE RESPONDENT EXPERIENCE WITH DESIGNING DIGITAL AND ANALOG VIDEO SECURITY SYSTEMS

In the early days of CCTV, large bulky cameras delivered an analog signal through coaxial cable to a video recorder, where grainy black and white images were recorded on a VHS tape. Tapes were often unchanged, and cameras were susceptible to weather, bright light, and darkness. Image recovery was a tedious process involving rewinding and fast-forwarding the tape until the event could be found.

In 2020, all of that has changed. Cameras are digital, images are high resolution, and analytics make the camera an active tool, able to alert security in an emergency. Images can be stored almost indefinitely and searching an event can be done in a few clicks of a mouse. For this reason alone, most security cameras that have not been updated in several years need to be reviewed and updated to be the most current technology.

As an example, The U.S. Department of Interior Bureau of Land Management has 17 facilities throughout the state of Wyoming that required physical security enhancements to meet current DHS and Department of Interior (DOI) Physical Security Standards. iParametrics conducted assessments of existing facility security conditions for each facility (including CCTV, Access Control System and Duress Alarm System equipment, locations, wiring and power, and network connectivity) and developed risk-based designs for security improvements. The designs included:

- Drawings and equipment specifications for each CCTV, ACS, and DAS system
- Detailed cost estimates for each system at each facility
- Camera fields of vision
- Locations of security equipment, associated wiring runs, and electrical connections and incorporated recommendations for modifications or full replacement



DESCRIBE RECOMMENDED STRATEGY INCLUDING ON-SITE COORDINATION AND SUPPORT SERVICES, BEST PRACTICE CONSULTING OPTIONS AND PROFESSIONAL SERVICES.

In coordination with your project team, we will define the processes, functions, activities, physical boundaries (facilities and locations), and stakeholders included within the boundaries of the projects. Within seven days of award, or upon a mutually agreed schedule, our Program Manager will meet with the Iowa project team for the initial project meeting to discuss project coordination and communication and to finalize the required data elements for the study.

Sound management and technical principles, industry best practices, and the philosophy of quantifiable measurement of cost, schedule, technical performance, and quality management will form the basis for project delivery to the State. Upon initiation of a project, we will prepare a cost estimate and a Microsoft Project schedule and maintain the schedule throughout and up to the closeout of the project.

Our standard methodologies include arranging and conducting meetings as necessary and in conjunction with project milestones, which usually includes providing transcripts to participants within 72 hours.

Our approach is designed to develop risk-based designs for modern integrated systems. These outputs include:

- The development of preliminary design criteria based on the buildings and associated threats
- The development of preliminary design criteria using risk analysis
- Adjustments to the preliminary design criteria to reflect the risk analysis or the cost necessary to implement the design criteria
- Adjustments to the criteria as necessary according to the professional judgments of the team and based on local and regional considerations

Design criteria are the basis for defining a protective system that mitigates vulnerabilities to the buildings we need to protect. The criteria describe the assets associated with a facility, the threat to those assets, the level to which those assets are to be protected against the threat, and any constraints to the protective system design that may be imposed by the planning team.

For existing facilities, vulnerabilities are additional factors in establishing the design criteria. Those vulnerabilities are based on evaluating how existing conditions affect the protection of the identified assets against the identified threats to the applicable levels of protection, including physical characteristics, qualities, and operational considerations that restrict or dictate design of security features. Including security requirements with project criteria allows security to be addressed at the start of the project and to be integrated into the total design efficiently and cost-effectively.

Once the designer knows the objectives of the security system and what to protect against and whom, the next step is to design the new system or characterize and determine how best to integrate people, procedures, and equipment to meet the objectives of the system.



Once the system is designed or characterized, it must be analyzed and evaluated to ensure that it meets the physical protection objectives. The design must allow the combination of protection elements working together to assure protection rather than regarding each feature separately. Implementation of the design then addresses the systematic and integrated protection of assets in anticipation of crisis event.

We use industry standards, like ASIS, ANSI, NFPA, and other Commercial Best Practices design standards and strategies to provide protective systems to mitigate the effects of a postulated threat. They govern the application of construction, building support systems, equipment, manpower, and procedures. Specific design strategies and their nature vary with each threat. They may vary by the sophistication of the protective measures, the degree of protection provided, or the degree of damage a building will be allowed to sustain, among others. The specific design strategies reflect the degree to which assets will be left vulnerable after the protective system has been employed.

Our subject matter experts possess the skills to evaluate, design, and integrate existing security cameras with current technologies to provide a turnkey solution for our customers. Our engineers have conducted site assessments for numerous facilities to determine if current technologies used on site were capable of being integrated with new systems to provide a cost savings for the customer.

PROVIDE AN ESTIMATE OF STATE OF IOWA STAFF TIME REQUIRED TO COMPLETE THE SECURITY SYSTEM DESIGN, IF DIFFERENT THEN EXHIBIT II.

The estimate for Iowa staff time is six to 12 hours per facility. This includes meetings, interviews, and escorts (when required).

IDENTIFY ANY THIRD-PARTY RESPONDENTS INVOLVED IN RESPONDENT'S IMPLEMENTATION STRATEGY AND DESCRIBE THESE RELATIONSHIPS, IF DIFFERENT THEN EXHIBIT II.

To ensure our drawings are completed in full compliance with all applicable local standards, any drawings requiring a stamp/signature will be routed through a professional engineer in the jurisdiction where the work is to be completed.

IDENTIFY THE TYPES OF DELIVERABLES THAT WOULD BE PROVIDED AS A PART OF THIS SERVICE.

iParametrics has extensive experience supporting projects that include requirements for physical and electronic security system evaluation and design which covers all the devices, technologies and specialist materials for perimeter, external and internal protection and response. This includes everything from intrusion detection sensors and closed-circuit television to barriers, lighting and access control. Our experience includes assessing, designing, estimating cost and managing complex programs dealing with:

- Security and access control systems
- Video surveillance and archiving systems



- Badging and credentialing systems
- Communications and response systems
- Security system infrastructure such as fencing and barriers, fiber optic cable systems, electronic asset protection systems, and operations centers.

On many of our projects, iParametrics provides evaluation, design, costing and program management for recommended systems. Our approach is designed to capture and apply the inputs and outputs of the physical security assessment (PSA) or physical security risk assessment (PSRA) and develop risk-based designs for modern integrated systems. Our experience also includes managing the full lifecycle of construction including procurement, installation and commissioning of systems.

Typical deliverables could include the Physical Security Risk Assessment, Programming/Planning documents, Schematic Design documents, Design Development documentation, Construction Documentation as outlined below:

Schematic Phase

- Schematic level design drawings including single line diagrams for security system and notations as required to describe the fundamental design concept for the system
- System descriptions and locations:
 - Access Controls, Surveillance and Security Alarms
 - Panel Locations, rack and wall space requirements
- Preliminary Device Location Plans
- Narrative of Security Systems needs
- Scope of work narrative including outline of relevant specification sections
- Initial schedule and cost estimate

Design Development Phase

- Design development drawings
- Outline specification including specific relevant specification sections
- Riser Diagrams
- Equipment location Plans
- Electronic Security Equipment Closet Layout
- Emergency Phone Locations and type
- Updated schedule and cost estimate

Construction Document Phase

- Detailed specification
- Detailed equipment location plans
- Equipment schedules (including all device specifications and electronic security system specifications)



- Concealed and exposed raceways
- Wiring Diagrams (Show quantity, typed, and splice and termination locations)
- Installation Details (Will include field device installation details)
- Detailed Sequences of Operations
- Trade coordination diagrams showing clearly the responsibility of each trade contractor responsible for security
- Updated schedule and cost estimate





iParametrics

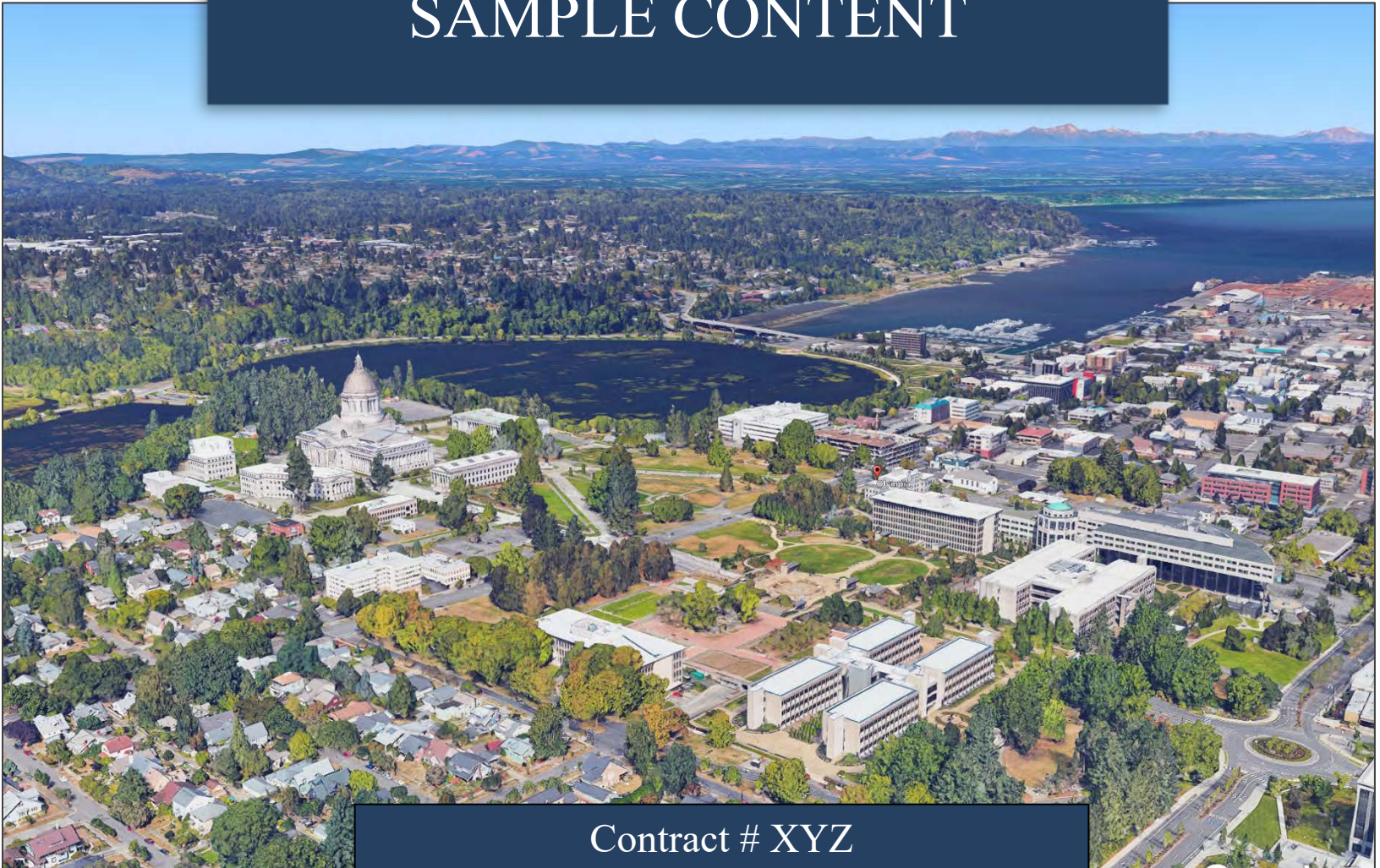


EXHIBIT 14- SAMPLE REPORTS



CONFIDENTIAL

Security Study of the SAMPLE CONTENT



Contract # XYZ
February 5, 2019

Prepared by:



This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

SAMPLE

THIS PAGE INTENTIONALLY LEFT BLANK

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

Table of Contents

1.	Background	4
2.	Executive Summary	5
3.	Risk Assessment Process	6
4.	Municipal Building	9
5.	Recreation Center	13
6.	Adult Center	16
	Appendix A – Design Basis Threat	18
	Appendix B - Facility Security Level Process and Site Worksheets	40
	Appendix C – Baseline Physical Security Standards	48
	Appendix D – Detailed Mitigation Strategies (including rough order of magnitude cost estimates).....	70
	Appendix E – References and Acknowledgements	79
	Appendix F – Acronyms	80
	Appendix G – Definitions.....	81
	Appendix H – Site Security Plans	83
	Appendix I – Proposed Location of Sensors and Cameras	84
	Appendix J - Lighting Survey.....	86
	Appendix K – Site Photos	88

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

1. Background

The Protection of Assets is a complicated and daunting task for any organization. When it extends to a Municipality the size of Anywhere with real property facilities, housing over 5,000 employees, and providing direct services to more than 3,000,000 city residents and visitors each day, that task can be overwhelming without adequate planning and resources. In order to accomplish the goals for the security of the City facilities there are four critical steps:

- Identify the assets to be protected,
- Identify the threats to be protected from,
- Develop standards for adequate protection, and
- Establish a Risk Management Process to ensure adequacy.

The city has taken initial steps to establish a security program; however, these actions have highlighted the need for a more consolidated and comprehensive strategy to ensure security management approaches that provide an adequate level of protection for all facilities in keeping with the city goals.

Therefore, the City of Anywhere has contracted with iParametrics, LLC to deliver a Security Risk Assessment Report that addresses the security risk based on requirements of each particular site as well as cost estimates and recommendations.

In accordance with the terms of the agreement, the assessment must include the following:

- A Security threat assessment to identify security related threats from internal and external sources during and after operating hours.
- Crime analysis.
- Identification of critical assets and pair most likely threats to identify most likely security scenarios on which to base the security program, analyze vulnerabilities, assess impacts of threat scenarios, identify actions that mitigate risk and provide an analysis of mitigation actions.
- A review of security staffing models and staffing levels at each site.
- A review of incident reports for the past two years.
- A physical evaluation of each site during and after operating hours.
- Review of security systems (access control, intrusion detection, video surveillance, lock and key control).
- Interviews with staff members.
- A physical evaluation of areas surrounding the buildings including loading docks, service areas, parking lots.
- A review of security related policies and procedures.
- A review of security training.
- A review of security related emergency response documents.
- A review of the City's mass notification capabilities.

This report is confidential; the disclosure of its contents would be contrary to the public interest.

This report is therefore unavailable for public inspection.

The Security Risk Assessment, cost estimates and recommendations include the following:

- Technical and physical security measures to mitigate or reduce risk to staff, information and physical assets (facilities) including specifications for any recommended system installations.
- Security Awareness programs intended to reduce victim assisted crimes.
- Modification to existing policies and procedures as appropriate.
- Initial incident response measures for security driven events.
- Implementation strategies with detailed security design cost estimates for recommended measures
- Two presentations to management to review findings and recommendations.

2. Executive Summary

In consultation with the Executive Management (EM) and key stakeholders, iParametrics conducted a security threat assessment of the existing security platform/posture. Throughout the week of November 5, 2018, the security specialists analyzed the Municipal Building, the Recreation Center and the Adult Center. The assessment included:

- Analysis of crime statistics and incident reports (Design Basis Threat (DBT) evaluation)
- Identification of critical assets
- Security staffing and organizational structure
- Review of security operations
 - Policies, plans and procedures
 - Building security systems installation and maintenance
 - Response force performance

The assessment team conducted over 125 interviews and visited the three facilities during operational hours and after hours. These visits allowed the team to review the physical security infrastructure of the properties, security training, emergency response documents and mass notification capabilities at each location. Detailed analysis of each facility is outlined in the following sections; however, here are our key observations.

- a. The city does not have a single point of contact for security or facility security related incidents. This has resulted in incomplete or nonexistent policies and procedures for the protection of critical assets. A tiered table of recommended physical security standards is included in Appendix C. The appointment/hiring of a properly trained person is necessary to develop staff and oversee implementation of the program.
- b. During normal operating hours visitors have uncontrolled access to staff and offices in most facilities. Balancing the need to provide a full host of services to the community, while still providing effective protection to employees and facilities is at the core of the risk

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

management program. Our facility-specific recommendations in Appendix D are designed to improve security while allowing public service to continue.

- c. The City does not have a centralized process for the reporting of security related incidents. Employees are doing a very good job of reporting incidents that rise to the level of criminal acts; however, incidents such as customer disputes, alarm failures or suspicious behavior are not routinely reported. A clearly defined reporting procedure will serve to enhance the baseline DBT provided in Appendix A.
- d. The facilities electronic security systems are monitored by three separate alarm monitoring centers under separate contracts by individual agencies. Utilization of separate alarm monitoring centers does not provide for the effective expenditure of city funds when compared to utilization of a single vendor who could provide a volume discount for the consolidation of the accounts. A cost savings assessment and detailed transition plan for this function must be developed.
- e. The City does not have a clear policy for the transportation and deposit of monetary instruments. As a result, employees and their personal automobiles are used for the pickup and transportation of monetary instruments from the city facilities to the bank. A detailed policy must be put into place to ensure the protection of staff and to reduce the liability of the City. If necessary, an armored car service may be contracted.
- f. The city lacks an operational mass notification system. Recommend that the city VOIP telephone system be upgraded to provide notification in emergencies.

3. Risk Assessment Process

Our process, which has been successfully implemented on several thousand government facilities, is in conformance with Interagency Security Committee (ISC) Risk Management Process for Government Facilities, ASIS SPC.1 and RIMS RA.1-2015, ISO3100, ISO/IEC 31010:2009. This methodology allows us to assess target value from the attacker perspective (essentially from the outside looking in), assess risk from the client perspective (essentially inside looking out) as well as give asset owners a roadmap forward in mitigating and recovering from an undesirable event.



Figure 3.1 – Risk Process and System Solution for Risk Assessment and Mitigation

Risk identification ascertains the sources and nature of risk and the effect of uncertainty on achieving the organization’s objectives. While this can be accomplished using a range of techniques for identifying the nature and sources of risk, they will all contain the following components, along with an understanding of the interplay between these components for a comprehensive identification and characterization of the associated risks:

- Asset and service identification, valuation, and characterization;
- Threat and hazard analysis;
- Vulnerability and capability analysis; and
- Criticality and impact analysis.

Our formula for the calculation of risk follows the equation:

$$\text{THREAT} \times \text{VULNERABILITY} \times \text{CONSEQUENCE (IMPACT)} = \text{RISK}$$

a. Developing the Design Basis Threat

Using the output from the asset identification, valuation and characterization phases we considered sources of risk that create uncertainty in achieving the City's objectives. We determined what are the threats and/or opportunities associated with potential risk events (risk pairings). The output of the threat analysis assessment is a comprehensive list of threats and opportunities focusing on prioritizing the most relevant to the achievement of objectives and an estimate of the likelihood of each threat occurring (i.e., an intentional/malevolent event or dependency/proximity hazard).

For Intentional/Malevolent Threats such as acts of vandalism, theft or terrorism, likelihood is based on the adversary's objectives and capabilities and the attractiveness of the region, facility, and threat/asset pairing relative to alternative targets. We worked directly with the DHS Fusion Center, the State Department of Public Safety and the law enforcement officials from Anywhere, USA and Anywhere County to leverage knowledge of threat intelligence from our Federal Risk Programs to develop clear postulated threat data based on real world statistics and intelligence to create a comprehensive list of specific human threats and their likelihood of occurring to the City and its critical assets.

The full DBT can be found in Appendix A.

b. Making the Facility Security Level (FSL) Determination and Vulnerability Analysis

The FSL determinations for City facilities direct the user to a set of baseline standards customized to address site-specific conditions. It applies to all facilities whether City-owned or leased, to be constructed, modernized, or purchased. This determination serves as the basis for implementing protective measures under the prescribed security criteria and standards. The FSL determination ranges from a Level I (lowest risk) to Level III (highest risk). Five key factors are taken into consideration when determining the FSL:

- Mission Criticality
- Symbolism
- Facility Population (to include visitors)
- Facility Size
- Threat to Tenants

The Municipal Building assessment determined it to be a Level III, indicating that the facility requires a HIGH Level of Protection (LOP). The Recreation Center and Adult Center assessment determined them to be a Level II, indicating that these facilities require a MEDIUM LOP. The FSL should be reviewed and adjusted, if necessary, as part of each initial and recurring risk assessment.

Complete FSL Worksheets for each facility are located in Appendix B.

c. Impact Analysis

Impact and Consequence Analysis provides a measurement of impact (both criticality and consequence) of the undesirable events relative to an organization's operation. It measures the impact of what losing a tangible or intangible asset, activity, or function will have on the operations of the organization.

The criticality of an asset, activity, or function can be intrinsic or derivative. The intrinsic criticality indicates the direct value of the asset, activity, or function in achieving the objectives of the organization. The derivative criticality indicates the indirect consequences of the risk event, and how the resultant consequences, indirectly related to the asset, activity, or function, will affect the organization in achieving its objectives. We considered the following elements in evaluating impact:

- The value of the asset to on-going operations and value generation;
- The value of the asset to internal and external stakeholders;
- Timeframe of criticality – the time period an asset can be unavailable before effects are significant;
- Relational affects: the effect on other assets and processes; and
- Public Relations: the impact on brand, image and reputation.

4. Municipal Building



The Municipal Building is located on a 20-acre site, in the central downtown area of Anywhere. The area is a mix of professional offices, retail businesses, medical offices, a city park and private residences. The building is a multi-story, single-tenant structure built primarily of steel, prefabricated concrete panels, brick and glass panels with a roof composed of steel supports, metal roofing material or a rubberized membrane. The facility is normally occupied from 6:00 a.m. to 6:00 p.m. Monday through Friday. Parking is located on the south side of the facility and in the underground parking garage to the north. Most parking areas are not actively monitored.

a. Facility Assets

- Police Department
- Municipal Court
- City Council Chambers
- City IT Data Center
- City Administration Offices
- Mailroom
- Emergency Generator

b. Site/Perimeter Security

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

There is limited perimeter security for the site. The south side of the facility is susceptible as a high-speed avenue of approach. The facility gas main is not protected. The facility HVAC system, commercial electric utilities are in an unlocked utility room on the west side of the facility. The emergency generator is protected by a concrete block wall and a locked metal gate in the building underground parking deck. When activated the exterior lighting affords adequate illumination for the facility (Appendix J – Lighting Survey).

c. Access Control/Entrances

The City of Anywhere provides direct service to the public at this location. Visitors to the administrative portions of the facility are directed to the first floor public lobby. The lobby is staffed with a receptionist during most public service hours. Visitors are not screened nor are they typically escorted while on site. Visitors have direct access to most employee work areas. Access to the building elevator is from the first floor public lobby.

The facility access control consists of an electronic Access Control System (ACS) and manually keyed locks. Doors not equipped with card readers are accessible by manually keyed locks. Authorized employees approved for access are issued a proximity card or a key for access as required by their job position.

The Municipal Building has fifteen perimeter entrances and exits. The east and west employee entrances, the public entrance, the court employee entrance, the police department public entrance, the police department employee entrance, the police department detention center entrance and the underground parking deck and six emergency exits. Most doors are operating properly with the exception of two emergency exits.

d. Security Forces and Response

The Anywhere Police Department provides law enforcement response with an estimated response time is less than 5 minutes. On Monday, Tuesday, Wednesday and Thursday during scheduled court hours three-armed court security officers are posted outside the first-floor public entrance to the Court. A Police Officer is posted in the City Council Chambers during public City Council meetings. There is no guard service for the administration portions of the facility.

e. Electronic Security Systems

The facility Electronic Security Systems (ESS) consists of an Intrusion Detection System (IDS), a Duress Alarm System (DUR), an ACS and a Closed Circuit Television (CCTV) system. The systems are integrated into the facility Security Management System and are monitored by a contracted central monitoring agency.

The IDS includes the magnetic switches covering the perimeter doors and any interior door equipped with a proximity card reader. The opened or closed status of the doors is reported by the system. The ground floor windows are not protected.

*This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.*

The Municipal Court, City Council Chambers, Police Department, Receptionist and some administrative areas are equipped with duress alarm buttons mounted to the underside of the employee desks or kick duress plates.

The ACS is controlled by ABC Security with oversight by the City Manager. Authorized employees are issued a proximity card for access when they are on-boarded through Human Resources. Employees are issued a key for interior offices access as required. Credentials can be immediately deleted from the ACS when access has been revoked or compromise is suspected.

The CCTV system consists of 62 cameras covering portions of the building perimeter, parking areas, some perimeter doors, the first-floor lobby and elevator, the interior of the entrance to the first-floor admin area and the City Council Chamber. There is a 45-day digital archive of all CCTV images.

f. Operational Security and Planning

There is no site-specific facility security plan. The EM is currently developing a city-wide Physical Security Plan.

g. Risk Analysis

The overall Risk Level of this facility is rated as Low.

Undesirable Event	Threat	Vulnerability	Impact	Risk
Assault	Medium	Low	Low	Low
Kidnapping	Medium	Low	Low	Low
Robbery	Medium	Low	Low	Medium
Theft	High	Low	Low	Medium
Vandalism	Medium	Low	Low	Low
Civil Disturbance	Medium	Low	Low	Low
Workplace Violence	Medium	Low	Low	Low
Insider Threat	Medium	Low	Low	Low
IED - Mailed or Delivered	Medium	Low	Low	Low
IED - Man Portable	Medium	Low	Low	Low
VBIED	Medium	Low	Low	Medium
Arson	Medium	Low	Low	Low
Ballistic Attack - Active Shooter	Medium	Low	Low	Low
Ballistic Attack - Small Arms	Medium	Low	Low	Low
Unauthorized Entry	Medium	Low	Low	Low
Disruption Of Facility or Security System	Medium	Low	Low	Low

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

Undesirable Event	Threat	Vulnerability	Impact	Risk
CBR Release - Internal	Medium	Low	Low	Low
CBR Release - Mailed or Delivered	Medium	Low	Low	Low
Release of Onsite Hazardous Material	Low	Low	Low	Low
Vehicle Ramming	Medium	Low	Low	Low

Figure 4.1 - Human Threat Risk Matrix

Undesirable Event	Threat	Vulnerability	Impact	Risk
River Flood	Low	Low	Low	Low
Coastal Flood	Low	Low	Low	Low
Seismic Hazard	Low	Low	Medium	Low
Tsunami	Low	Low	Low	Low
Windstorm	Low	Low	Low	Low
Hailstorm	Low	Low	Low	Low
Tornado	Low	Low	Medium	Low
Wildfire	Low	Low	Low	Low
Lightning	Medium	Medium	Medium	Medium
Volcano	Low	Low	Low	Low

Figure 4.2 –Environmental Threat Risk Matrix

h. Findings and Observations

Critical Vulnerabilities:

- Facility utilities are unprotected.
- Perimeter of building not protected from high speed avenue of approach.
- Uncontrolled access to staff/offices.
- Parking security (not segregated or protected).
- Courtroom and City Council Chamber security.
- IT Data center that houses the Security Management System is not properly protected.
- No dedicated safe/money-count room.
- Lack of adequate duress buttons.
- Lack of adequate CCTV coverage of facility and quality of images (Analog).
- Lack of adequate IDS coverage for the facility.

Detailed mitigation strategies and cost estimates can be found in Appendix D.

5. Recreation Center



The Recreation Center is located on a 35-acre site, 2 miles north of the Municipal Building. The area is a mix of city and county parks and private residences. The building is a multi-story, single-tenant structure built primarily of steel, concrete block, brick and glass panels with a roof composed of steel supports, metal roofing panels, an EMPT membrane. The facility is open to the public from 5:00 a.m. to 8:00 p.m. Monday through Thursday, 5:00 a.m. to 7:00 p.m. Friday, 7:00 a.m. to 7:00 p.m. Saturday, and is closed on Sunday. Parking is located on the north and west side of the facility. Access to the parking areas is uncontrolled.

a. Facility Assets

- Children's Pavilion
- Pump Room
- IT Data Room
- Administration Offices
- Mailroom

b. Site/Perimeter Security

There is 6-foot high privacy fencing on the west and portions of the north perimeter. There is no perimeter security on the south and east side of the facility. The facility commercial electric utilities are unprotected on the northwest side of the facility. When activated the exterior lighting affords limited illumination for the facility (Appendix F – Lighting Survey).

c. Access Control/Entrances

The City of Anywhere provides direct service to the public at this location. Visitors access the facility from the public entrance on the north side of the building. The lobby is staffed with up to three receptionist/cashiers during peak public service hours located inside the public lobby. Visitors are not screened nor are they escorted while on site. Access to the building elevator is from the north hallway adjacent the gym.

Access control consists of an electronic ACS and manually keyed locks. Doors not equipped with card readers are accessible by manually keyed locks. Authorized employees approved for access are issued a proximity card or a key for access as required by their job position.

The Recreation Center has 19 perimeter entrances and emergency exits. The public entrance, the kitchen exit, four community room exits, community room hallway exit, southeast patio doors, mechanical room, storage room, west emergency exit, west stairwell emergency exit, maintenance vehicle overhead door, maintenance personnel door, sprinkler control room, two

emergency exits from the gym, employee entrance, and the children’s pavilion door. All doors are operating properly.

d. Security Response

Law Enforcement response is provided by the Anywhere Police Department with an estimated response time of 4 minutes.

a. Electronic Security Systems

The facility is equipped with an IDS, an ACS and a CCTV system. The systems are integrated into the Security Management System monitored by the Acme Security Monitoring Center.

The IDS provides coverage of the perimeter doors, critical interior rooms and hallways. Most ground floor windows are not protected by the IDS.

The ACS is controlled by Acme Security with direct oversight by Management. Authorized employees are issued a proximity card for access when they are on-boarded through Human Resources. Employees are issued a key for interior offices access as required. Credentials can be immediately deleted from the ACS when access has been revoked or compromise is suspected.

The CCTV system consists of an onsite Network Video Recorder (NVR) and 17 cameras. The system covers portions of the northwest and south parking areas, pool area, children’s pavilion, public lobby, hallway outside the men’s and lady’s locker room, east and west gym area, admin area where mail is processed, front desk, game room, community rooms hall, pool areas, the second hallways, and the exterior of the public entrance. There is a 30-day digital archive of all CCTV images. The system is capable of local monitoring however; the computer utilized to view the system is non-operational due to lack of adequate software updates and compatibility issues.

e. Operational Security and Planning

There is no site-specific facility security plan. The MT is currently developing a city-wide Physical Security Plan. The Parks and Recreation division have established emergency plans for medical emergencies, and some security procedures.

f. Risk Analysis

The overall Risk Level of this facility is rated as Low.

Undesirable Event	Threat	Vulnerability	Impact	Risk
Assault	Medium	Low	Low	Low
Kidnapping	Medium	Low	Low	Low
Robbery	Medium	Low	Low	Medium
Theft	High	Low	Low	Medium

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

Undesirable Event	Threat	Vulnerability	Impact	Risk
Vandalism	Medium	Low	Low	Low
Civil Disturbance	Medium	Low	Low	Low
Workplace Violence	Medium	Low	Low	Low
Insider Threat	Medium	Low	Low	Low
IED - Mailed or Delivered	Medium	Low	Low	Low
IED - Man Portable	High	Low	Low	Medium
VBIED	Medium	Low	Low	Low
Arson	Medium	Low	Low	Low
Ballistic Attack - Active Shooter	Medium	Low	Low	Low
Ballistic Attack - Small Arms	Medium	Low	Low	Low
Unauthorized Entry	Medium	Low	Low	Low
Disruption Of Facility or Security System	Medium	Low	Low	Low
CBR Release - Internal	Medium	Low	Low	Low
CBR Release - Mailed or Delivered	Medium	Low	Low	Low
Release of Onsite Hazardous Material	Low	Low	Low	Low
Vehicle Ramming	Medium	Low	Low	Low

Figure 5.1 - Human Threat Risk Matrix

Undesirable Event	Threat	Vulnerability	Impact	Risk
River Flood	Low	Low	Low	Low
Coastal Flood	Low	Low	Low	Low
Seismic Hazard	Low	Low	Medium	Low
Tsunami	Low	Low	Low	Low
Windstorm	Low	Low	Low	Low
Hailstorm	Low	Low	Low	Low
Tornado	Low	Low	Medium	Low
Wildfire	Low	Low	Low	Low
Lightning	Medium	Medium	Medium	Medium
Volcano	Low	Low	Low	Low

Figure 5.2 –Environmental Threat Risk Matrix

g. Findings and Observations

Critical Vulnerabilities:

- The facility has experienced uncontrolled access from perimeter doors being propped-open.
- Gates to the pool can be opened from the exterior.
- Positive control to the Children’s Pavilion interior door has not been established.
- The facility IDS does not provide complete coverage of the facility.
- The CCTV monitoring station at the front desk is not operating properly due to upgrade of the IT equipment.
- All perimeter doors and the money-count room are not covered by the CCTV system.

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

- Several perimeter and interior are not equipped with ACS and are critical areas or used by staff frequently.
- Several key locations are not equipped with duress buttons.

Detailed mitigation strategies and cost estimates can be found in Appendix D.

6. Adult Center



The Anywhere Adult Center is located on a 7.25-acre site, 1 mile east of the Municipal Building. The area is a mix of a church, private residences, and city park. The building is a multi-story, single-tenant structure built primarily of wood studs, brick and glass panels with a roof composed of steel supports, metal roofing panels, an EMPT membrane. The facility is open to the public from 8:30 a.m. to 4:00 p.m. Monday through Friday and on Saturday and Sunday as needed. Parking is located on the southwest and southeast sides of the facility. Access to the parking areas is uncontrolled and not all areas are monitored with CCTV coverage.

a. Facility Assets

Staff Offices
IT Data Room

b. Site/Perimeter Security

There is no perimeter security for the facility. When activated the exterior lighting affords minimum illumination for the facility (Appendix J – Lighting Survey).

c. Access Control/Entrances

The City of Anywhere provides direct service to the public at this location. Visitors access the facility from the public entrance on the west and east side of the building. The lobby is staffed with a receptionist/cashier. Visitors are not screened nor are they escorted while on site.

Access control consists of an ACS and manually keyed locks. Doors not equipped with card readers are accessible by manually keyed locks. Authorized employees approved for access are issued a proximity card or a key for access as required by their job position.

The Center has six perimeter entrances and exits. The public entrance, the employee entrance, the kitchen exit, Prospect Hall emergency exit, the east building entrance, and the Aloha Room emergency exit. All doors are operating properly.

d. Security Response

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

Law Enforcement response is provided by the Anywhere Police Department with an estimated response time of 4 minutes.

a. Electronic Security Systems

The facility is equipped with an IDS, an ACS and a CCTV system. The systems are integrated into the Security Management System monitored by Central Security.

The Central Security monitors the status of the perimeter doors and any interior door equipped with a proximity card reader as well as the motion sensor. The opened or closed status of the doors is reported by the system. Some ground floor windows are not protected by the Intrusion Detection System (IDS).

The ACS is controlled by Acme Security with direct oversight by the site manager. Authorized employees are issued a proximity card for access when they are on-boarded through Human Resources. Employees are issued a key for interior offices access as required. Credentials can be immediately deleted from the ACS when access has been revoked or compromise is suspected.

The CCTV system consists of five (5) IP cameras covering the west public and employee entrance, the public lobby, the interior of the east hallway entrance, the interior of prospect hall and the northwest parking area. CCTV images are not monitored onsite. There is no local archive of the facility CCTV system. The cameras images are transmitted via a CCTV VLAN on the city IT network back to the Municipal Building for digital archival. There is a 30-day digital archive maintained of the CCTV images.

e. Operational Security and Planning

There is no site-specific facility security plan. The MT is currently developing a city-wide Physical Security Plan. The Parks and Recreation division have established emergency plans for medical emergencies, and some security procedures.

f. Risk Analysis

The overall Risk Level of this facility is rated as Low.

Undesirable Event	Threat	Vulnerability	Impact	Risk
Assault	Medium	Low	Low	Low
Kidnapping	Medium	Low	Low	Low
Robbery	Medium	Low	Low	Medium
Theft	High	Low	Low	Medium
Vandalism	Medium	Low	Low	Low
Civil Disturbance	Medium	Low	Low	Low
Workplace Violence	Medium	Low	Low	Low
Insider Threat	Medium	Low	Low	Low

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

Undesirable Event	Threat	Vulnerability	Impact	Risk
IED - Mailed or Delivered	Medium	Low	Low	Low
IED - Man Portable	High	Low	Low	Medium
VBIED	Medium	Low	Low	Low
Arson	Medium	Low	Low	Low
Ballistic Attack - Active Shooter	Medium	Low	Low	Low
Ballistic Attack - Small Arms	Medium	Low	Low	Low
Unauthorized Entry	Medium	Low	Low	Low
Disruption Of Facility or Security System	Medium	Low	Low	Low
CBR Release – Internal	Medium	Low	Low	Low
CBR Release - Mailed or Delivered	Medium	Low	Low	Low
Release of Onsite Hazardous Material	Low	Low	Low	Low
Vehicle Ramming	Medium	Low	Low	Low

Figure 6.1 - Human Threat Risk Matrix

Undesirable Event	Threat	Vulnerability	Impact	Risk Score
River Flood	Low	Low	Low	Low
Coastal Flood	Low	Low	Low	Low
Seismic Hazard	Low	Low	Medium	Low
Tsunami	Low	Low	Low	Low
Windstorm	Low	Low	Low	Low
Hailstorm	Low	Low	Low	Low
Tornado	Low	Low	Medium	Low
Wildfire	Low	Low	Low	Low
Lightning	Medium	Medium	Medium	Medium
Volcano	Low	Low	Low	Low

Figure 6.2 –Environmental Threat Risk Matrix

g. Findings and Observations

Most prevalent risks:

- The facility has excessive plant/vegetation growth around the perimeter of the building CEPTD.
- Visitors frequently propped-open perimeter doors without notifying management or employees.
- The CCTV system does not efficiently cover the parking lot and building perimeter.
- The kitchen and east building perimeter doors are frequently used by staff and should be equipped with ACS.

Detailed mitigation strategies and cost estimates can be found in Appendix D.

Appendix A – Design Basis Threat

1.0 Background

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

Anywhere, USA is a county seat located in Somewhere County. As of 2016, the population was 391,372, an increase of 4% as of 2010. The city has a total area of 856 square miles with a population density of 3,505 people per square mile. It borders other communities on all sides including Maplesville to the north, Oakville to the east, Lakeview to the west, and Apollo to the south.

The City has over 5,000 employees working in several facilities throughout the City. Some employees work in jobs requiring them to work outside of City controlled facility and interact with the community on a face-to face basis. These interactions include site visits, facility inspections and delivery of services. The remainder of City employees works in forward facing offices where face to face contact with customers is essential to the mission of serving the community. The vast majority of these exchanges occur without incident even in some of the most serious cases. However, in a small number of these cases, the contact becomes hostile, threatening and occasionally dangerous. The threats addressed in this report are those most likely to occur in and around City employees, facilities and customers.

1.1 Acknowledgements

The following Design Basis Threat is based on, and in certain cases excerpted from documents and information provided by:

- Department of Homeland Security Interagency Security Committee,
- Federal Bureau of Investigation Uniform Crime Reporting,
- Department of Homeland Security Fusion Center,
- Anywhere Police Department,
- Surrounding law enforcement agencies and
- Incident Reports from multiple City departments.

2.0 Applicability and Scope

This report is applicable to all buildings and facilities in Anywhere, USA occupied and/or managed by City employees for department activities. Management officials, security organizations, and working groups should reference the most current edition of the DBT, unless a current agency-specific threat assessment publication addressing the Undesirable Events is available.

The DBT is an estimate of the threat City operations face across a range of Undesirable Events and is based on the best intelligence information, assessments, incident reports and crime statistics available at the time of publication. Users of the DBT must consider that undiscovered plots may exist, adversaries are always searching for new methods and tactics to overcome security measures, and the lone adversary remains largely unpredictable.

3.0 Definitions (Listed by relationship to each other)

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

For the purposes of this report, the following definitions apply. For ease of comparison, the definitions are grouped according to relationship to each other.

Design-Basis Threat (DBT): A profile of the type, composition, capabilities, methods (tactics, techniques, and procedures), and the goals, intent, and motivation of an adversary upon which the security engineering and operations of a facility are based.

Baseline Threat: The estimate of the relative threat posed to a City facility from an Undesirable Event. Baseline threat is categorized as Low, Medium or High.

Undesirable Event: An incident directed towards a City facility that adversely impacts the operation of the facility, the mission of the agency, or personnel.

Facilitating Event: An activity or action associated with the pre-planning or preparation for an event, which potentially increases the likelihood of success of an Undesirable Event by making it less difficult to achieve and/or assisting its progress.

Level of Protection (LOP): The degree of security provided by a particular countermeasure or set of countermeasures. Levels of Protection used in this Standard are Low, Medium and High.

Level of Risk: The combined measure of the threat, vulnerability, and consequences posed to a facility from a specified Undesirable Event.

Risk: A measure of potential harm from an Undesirable Event that encompasses threat, vulnerability, and consequence.

Threat: The intention and capability of an adversary to initiate an Undesirable Event.

Vulnerability: A weakness in the design or operation of a facility that can be exploited by an adversary.

Consequence: The level, duration, and nature of the loss resulting from an Undesirable Event.

4.0 How to Apply This Report

The DBT establishes the characteristics of the threat environment to be used in conjunction with all baseline physical security standards.

The intent of the DBT is three-fold:

- To inform the deliberations of working groups as they establish standards.
- To support the calculation of the threat, vulnerability, and consequence to a facility when calculating risk to a City facility and determining an appropriate Level of Protection, particularly when applying Physical Security Criteria.

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

- To determine specific adversary characteristics that performance standards and countermeasures are designed to mitigate.

4.1 Standard Development

As the City leaders develop standards to address threats against City facilities, they must have a clear understanding of the threat they are trying to counter. Security professionals should use the DBT as the basis for quantifying and characterizing threats in general.

For example, requirements for response force training, equipment, and weapons should be based on the DBT's postulated adversary capabilities for such events as robbery, assault, workplace violence, ballistic attacks, etc. In the case of graduated standards increasing levels of protection should be based on descriptions of factors that heighten the threat or increase the intensity of the event for higher-risk facilities.

4.2 Risk Assessments

The DBT provides specific details as to the characteristics of each event that might take place at a City facility. They are based on a worst-reasonable-case scenario. Each event provides sufficient information from which the threat, consequences, and vulnerability can be estimated in the conduct of a risk assessment.

4.3 Baseline Threat Level Ratings:

LOW: A low rating generally means there is an EXISTENCE and a CAPABILITY of a factor that indicates the likelihood of a threat, weapon, and tactic being used against City facilities is possible. There may or may not also be a HISTORY for the same.

MEDIUM: A medium rating generally means there is an EXISTENCE, CAPABILITY, and HISTORY of a factor that indicates the likelihood of a threat, weapon, and tactic being used against City facilities is possible. There may or may not also be INTENTIONS for the same.

HIGH: A high rating generally means there is an EXISTENCE, CAPABILITY, HISTORY, and INTENTIONS of a factor that indicates the likelihood of a threat, weapon, and tactic being used against City facilities is expected. There may or may not also be TARGETING for the same.

5.0 Undesirable Events

This section lists the Undesirable Events that could have an adverse impact on the operation of a facility or mission of a City agency.

Undesirable Event	Rating
Assault - Physically assaulting (with or without a weapon) a person or person inside the facility or on the property. Includes the crimes of homicide, aggravated assault and rape.	LOW
Kidnapping - Abduction of an occupant or visitor from a facility, including from inside secured areas (e.g., a child care center) or outside on the site (e.g., a City-controlled parking lot).	LOW/MEDIUM
Robbery - Unlawful taking of City-owned or personal property from an employee or other person(s) by force or threat of force. The incident could occur inside or outside of a facility.	MEDIUM
Theft - Unauthorized removal of City-owned or personal property from a facility.	MEDIUM
Vandalism - To willfully or maliciously destroy, injure, disfigure, or deface any public or private property, real or personal, without the consent of the owner or person having custody or control by cutting, tearing, breaking, marking, painting, drawing, covering with filth, or any other such means as may be specified by local law.	LOW
Civil Disturbance - Deliberate and planned acts of violence, destruction or denial of access stemming from organized demonstrations on or near City property.	LOW
Workplace Violence - Violence perpetrated by an authorized occupant or an employee. The assailant can be another employee, authorized tenant, or an authorized visitor.	LOW
Insider Threat - Individuals with the access to and/or inside knowledge of an organization that would allow them to exploit the vulnerabilities of the entity's security, systems, services, products, information, or facilities with the intent to cause harm.	LOW
Explosive Device - Mailed or Delivered - An explosive device sent to the facility through U.S. Mail or a commercial delivery service, including an unwitting courier.	LOW
Explosive Device - Man-Portable - An explosive device concealed in a backpack, briefcase or other innocuous container which is capable of being carried by a single operative, and placed outside of a secure area, near an entrance to the facility or carried into a facility by an adversary or an unsuspecting occupant, visitor or courier and left to detonate after the adversary departs.	MEDIUM
Explosive Device – Vehicle Borne Improvised Explosive Device (VBIED) – An attack that utilizes a vehicle to deliver an improvised explosive device against a facility. A passenger sedan containing an IED with a 50-200 pound (TNT equivalent) explosive main charge, utilizing a remote control, timed, or victim operated trigger.	LOW
Arson - Deliberately or attempting to set fire in or around a facility or associated grounds and assets.	LOW

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

Undesirable Event	Rating
Active Shooter - An active shooter is an individual actively engaged in killing or attempting to kill people in a confined and populated area, typically through the use of firearms.	LOW
Ballistic Attack - Small Arms - One or more individuals armed with small arms fire Small Arms indiscriminately at a facility from outside.	LOW
Unauthorized Entry - Unauthorized access to a facility or controlled area by forced entry or surreptitiously by stealth. Includes the use of deceit, coercion, or social engineering to gain access to a facility through a controlled entrance.	LOW
Disruption of Facility or Security Systems - Physically accessing facility or security systems for the purpose of disruption or manipulation of the systems.	LOW
CBR Release - Internal - Intentional release of a CBR agent carried into the facility, including in general interior spaces (lobbies) or into specific rooms or systems (HVAC rooms).	LOW
CBR Release - Mailed or Delivered - A CBR substance or dispersal device sent to the facility through U.S. Mail or a commercial delivery service, including an unwitting courier.	LOW
Release of Onsite Hazardous Materials - Unauthorized access to hazardous materials stored onsite with the intent of harming personnel or damaging the facility.	LOW
Vehicle Ramming - Driving a vehicle in an attempt to penetrate a facility (e.g., lobby or loading dock) or breach a defined perimeter.	LOW

Undesirable Event	5.1 Assault				
Definition	Physically assaulting (with or without) a person or person inside the facility or on the property. Includes the crimes of homicide, aggravated assault and rape.				
Original Assessment	8/1/2017	Revision	1	Date	8/1/2018

5.1.1 Baseline Threat

Based on nationwide, regional and Anywhere crime statistics and the frequency of events at City facilities, the baseline threat to City facilities from this event is assessed to be LOW.

Anywhere ended 2017, with a 34% increase in Index Offenses compared to 2016. However violent crime decreased by 3%.

- 1 homicide was reported compared to 0 in 2016.
- 32 robberies were reported compared to 20, resulting in an increase of 16.6%.

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

- 14 rapes were reported compared to 12, resulting in an increase of 14.3%.
- 53 aggravated assaults were reported compared to 71, resulting in a decrease of 25.3%.

In 2015, there were an estimated 764,449 aggravated assaults in the nation and 8,685 in the state, 3,413 in the region and only 53 locally. The FBI’s UCR Program defines aggravated assault as an unlawful attack by one person upon another for the purpose of inflicting severe or aggravated bodily injury. The UCR Program further specifies that this type of assault is usually accompanied by the use of a weapon or by other means likely to produce death or great bodily harm. Attempted aggravated assault involving the display of—or threat to use—a gun, knife, or other weapon is included in this crime category because serious personal injury would likely result if the assault were completed. When aggravated assault and larceny-theft occur together, the offense falls under the category of robbery.

5.1.2 Outlook

It is anticipated that violent crime levels will increase in accordance with the upward trend of the last two years. It is important to identify that this is not an absolute outlook and many of the contributing factors to crime could exacerbate circumstances and increase activity. Areas with high population density, transient populations, or public services are likely to sustain existing statistical rates. Practitioners should evaluate the many contributing factors of criminal activity for the given target areas of assessment to determine the causal factors and design protective postures accordingly.

Undesirable Event	5.2 Kidnapping				
Definition	Abduction of an occupant or visitor from a facility, including from inside secured areas (e.g., a child care center) or outside on the site (e.g., a Government-controlled parking lot).				
Original Assessment	8/1/2017	Revision	1	Date	8/1/2018

5.2.1 Baseline Threat

Based on the frequency of historical events, terrorism literature describing operational planning requirements, and disrupted plots, the baseline threat of an abduction of employees and officials at City facilities is assessed to be LOW.

Based on the frequency of historical events in general, the baseline threat of an abduction of a child at City facilities is assessed to be MEDIUM.

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

Kidnapping of City officials inside the U.S. is a rare occurrence, but attempts have been made in the past. International terrorist organizations and other criminal groups have sustained a continued interest in utilizing kidnapping as a means of capital gains and/or instill fear in targets.

According to the National Crime Information Center (NCIC), in 2014, 17,631 of 635,155 missing persons reported were listed as "missing involuntarily." This included 4,806 (27.3 percent) under the age of 18. In 2013, 18,841 of 627,911 missing persons were reported as "missing involuntarily," of which 4,883 (25.9 percent) were under the age of 18. Kidnapping makes up less than two percent of all violent crimes against juveniles reported to police. Based on the identity of the perpetrator, there are three distinct types of kidnapping:

- Kidnapping by a relative of the victim or "family kidnapping" (49 percent),
- Kidnapping by an acquaintance of the victim or "acquaintance kidnapping" (27 percent), and
- Kidnapping by a stranger to the victim or "stranger kidnapping" (24 percent).

Family kidnapping is committed primarily by parents, involves a larger percentage of female perpetrators (43 percent) than other types of kidnapping offenses, occurs more frequently to children under six, equally victimizes juveniles of both sexes, and most often originates in the home. Schools are an unusual site for abduction, even for family abductions. Only five percent of family abductions, four percent of acquaintance abductions, and three percent of stranger kidnappings occur at schools. Family abductions are most commonly carried out by only one perpetrator.

- 58,200 children were the victims of nonfamily abductions.
- 115 children were the victims of "stereotypical" kidnapping. These crimes involve someone the child does not know or a slight acquaintance that holds the child overnight, transports the child 50 miles or more, kills the child, demands ransom, or intends to keep the child permanently.

This information begins to inform a baseline establishment of the frequency of this event. The *America's Missing: Broadcast Emergency Response* (AMBER) alerts below provide additional insight into the geographical basis of these frequencies.

AMBER Alerts by State/Territory:

From January 1, 2015, to December 31, 2015, 182 AMBER Alerts were issued in 44 states. Texas issued the most AMBER Alerts with 15 percent, followed by California and Georgia with 7 percent each, and Colorado with 2 percent.

5.2.2 Outlook

The rate of criminally-motivated kidnapping is expected to remain constant for the foreseeable future. Kidnapping by drug and human smuggling organizations is also becoming popular in the Southwestern U.S. along the southern border. Incidences of stereotypical child abduction do not appear to be on the rise, and thus the trend is expected to remain relatively stable in the foreseeable future.

This report is confidential; the disclosure of its contents would be contrary to the public interest.

This report is therefore unavailable for public inspection.

Undesirable Event	5.3 Robbery				
Definition	Unlawful taking of Government-owned or personal property from an employee or other person(s) by force or threat of force. The incident could occur inside or outside of a facility.				
Original Assessment	8/1/2017	Revision	1	Date	8/1/2018

5.3.1 Baseline Threat

Based on nationwide crime statistics and the frequency of events at City facilities, the baseline threat to City facilities from this event is assessed to be MEDIUM.

In 2015, there were an estimated 327,374 robberies nationwide. 3,080 in the state, 1,503 in the region and 32 locally. The estimated number of robberies increased 1.4% nationally, 7.8% in the state, 17.4% regionally and 66 % locally from the 2014 estimate. The estimated robbery rate of 101.9 per 100,000 inhabitants in 2015 showed an increase of 0.6 percent when compared with the 2014 rate. The average dollar value of property stolen per reported robbery was \$1,190. Robberies accounted for an estimated \$390 million in losses. Banks experienced the highest average dollar loss at \$3,884 per offense.

Based upon this information, it appears the majority of robberies occur on public pathways or parking facilities. Information regarding the destination and origin of the victims was not provided, but it can be assumed that these incidents are more likely to occur when persons are in transit between locations.

5.3.2 Outlook

The 2015 statistics show the estimated volumes of violent crimes decreased 6.5 percent, when compared with the 2014 estimates. Practitioners should note that while the overall national rates have continued to decline, as indicated above some communities may have experienced sustained or increased rates based on a number of causal factors. Robberies have not presented an increased threat in City facilities when compared against other violent and property related incidents. Although an increase in robberies has been documented in Anywhere statistics, the overall number of facilities affected remains relatively low.

Undesirable Event	5.4 Theft				
Definition	Unauthorized removal of Government-owned or personal property from a facility.				
Original Assessment	8/1/2017	Revision	1	Date	8/1/2018

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

5.4.1 Baseline Threat

Based on nationwide, regional and Anywhere crime statistics and the frequency of events at City facilities, the baseline threat to City facilities from this event is assessed to be MEDIUM.

Anywhere ended 2017, with a 34% increase in Index Offenses compared to last year. Property crime increased by 37.5%.

- Burglary increased overall by 18.9%, (195 compared to 164).
- 215 vehicle thefts were reported compared to 108, resulting in an increase of 99.1%.
- 8 arson cases were reported compared to 5, resulting in an increase of 60%.

In 2015, there were an estimated 114,627 thefts in the state, 36,095 in the region and 4,482 locally. The FBI’s UCR Program defines larceny-theft as “the unlawful taking, carrying, leading, or riding away of property from the possession or constructive possession of another.” This includes thefts of bicycles, motor vehicle parts and accessories, shoplifting, pocket-picking, or the stealing of any property or article that is not taken by force and violence or by fraud. Attempted larcenies are included. Embezzlement, confidence games, forgery, checks fraud, etc., are excluded.

5.4.2 Outlook

While larceny/theft has decreased on a national level it is on the rise in the Anywhere Police Department area of responsibilities. As the City and surrounding areas continue to grow the numbers of thefts are expected to grow.

Undesirable Event	5.5 Vandalism					
Definition	To willfully or maliciously destroy, injure, disfigure, or deface any public or private property, real or personal, without the consent of the owner or person having custody or control by cutting, tearing, breaking, marking, painting, drawing, covering with filth, or any other such means as may be specified by local law. Includes attempts.					
Original Assessment	8/1/2017	Revision	1	Date	8/1/2018	

5.5.1 Baseline Threat

Based on nationwide, regional and Anywhere crime statistics regarding the frequency of random and directed events at City facilities, the baseline threat from this event is assessed to be LOW.

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

The National Crime Prevention Council reports that graffiti is the most common form of vandalism. Vandalism is often associated with juveniles and gangs, but is also a tactic used by typically nonviolent adversary organizations. When associated with an adversary group, it is often used to make a political statement. Approximately 80 percent of graffiti is gang or “tagger” related.

5.5.2 Outlook

In 2015, there were an estimated 7,993,631 property crime offenses in the nation, and 112,869 in the state, 36,095 in the region and 5,482 locally. The 2-year national trend showed that property crime offenses declined 2.6 percent in 2017 when compared with the 2016 estimate. The regional trend increased by 9.6 percent, where the local trend increased by 37 percent in 2017 when compared with the 2016 estimate. Analysis indicates that as the surrounding areas continue to grow the numbers of property crimes are expected to increase.

Undesirable Event	5.6 Civil Disturbance				
Definition	Deliberate and planned acts of violence and destruction stemming from organized demonstrations on or near City property.				
Original Assessment	8/1/2017	Revision	01	Date	8/1/2018

5.6.1 Baseline Threat

The frequency of organized protests at municipal facilities is medium; however, historically very few organized protests have turned particularly violent. Consequently, the baseline threat to City facilities from this type of event is assessed to be LOW.

Civil disturbance is typically started by a small cadre of offenders agitating peaceful assemblies engaging in lawful First Amendment activities. Most of the protest or demonstration activities are organized and well within the bounds of the federal, state, and local laws. Nevertheless, these demonstrations have the potential to conceal particularized offenders seeking to incite violence and property damage. 2017 and 2016 have had numerous incidents of civil unrest documented throughout the United States. The majority of this activity developed from peaceful First Amendment events targeting policy changes in law enforcement. Police techniques and specifically, use of force policies and application continue to receive national media attention. Incidents involving police action continue to polarize communities and spark political debates on a national scale. Consequently, large groups of citizens are peacefully assembling to persuade City leaders to get involved.

5.6.2 Outlook

Organized demonstrations at Federal, State and City facilities are expected to continue on a routine basis, and some are likely to turn into violent civil disturbances with unpredictable

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

regularity. Major periods of increased national policy activity will sustain increased activist interest. Increased polarization on policy issues increases the probability of legal demonstrations. Frequent legal demonstrations or increased occurrence have the inherent possibility to become disturbances if subjected to influences of nefarious actors and group dynamics.

Undesirable Event	5.7 Workplace Violence				
Definition	Violence perpetrated by an authorized occupant on an employee. The assailant may be another employee, authorized tenant, or an authorized visitor.				
Original Assessment	8/1/2017	Revision	1	Date	8/1/2018

Note: Workplace violence is often defined as any violence occurring in the workplace. The majority of the Undesirable Events addressed in the DBT document are forms of violence against employees, and thus all might be categorized “workplace violence.” For the purposes of the DBT, “workplace violence” is limited to violence between co-workers. Other events address other violence which may be perpetrated against employees, including criminal and terrorist attacks.

5.7.1 Baseline Threat

Based on the overall workplace violence statistics in the United States and State of Colorado, to include various types of assault, abuse, and harassment, the baseline threat to City facilities from this event is assessed to be LOW.

5.7.2 Outlook

The number of workplace homicides and violent crime incidents has continued to gradually decline over the last 20 years. UCRs indicate decreases as well as labor statistics collected on fatalities in the workplace. The ISC anticipates the statistical pattern reflected over the last 20 years will continue unless there is a significant aggregation or shift in contributing factors.

Undesirable Event	5.8 Insider Threat				
Definition	Individuals with the access to and/or inside knowledge of an organization that would allow them to exploit the vulnerabilities of that entity’s security, systems, services, products, information, or facilities with the intent to cause harm. This includes exploiting vulnerabilities of cyber systems.				
Original Assessment	8/1/2017	Revision	1	Date	8/1/2018

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

5.8.1 Baseline Threat

The presence of a complicit, potentially disgruntled insider likely increases the threat of other Undesirable Events. The baseline threat to City facilities from this activity is assessed to be LOW.

In most instances to date, the insider threat has been largely limited to criminal acts of theft and espionage, with some evidence of sabotage. Information from several recent planned or thwarted terrorist plots shows the importance of the use of insiders to gain access to targets and collect preoperational information.

5.8.2 Outlook

The insider threat will continue to pose a significant challenge to disrupting adversary acts in the future. Rapidly escalating technology and network risks are combining with growing globalization of workforces, supply chains, and service providers to produce new threats and risks.

Undesirable Event	5.9 Explosive Device — Mail or Delivery				
Definition	An explosive device sent to the facility through U.S. Mail or a commercial delivery service.				
Original Assessment	8/1/2017	Revision	1	Date	8/1/2018

5.9.1 Baseline Threat

Based on the nature of the attack, availability of components and instructions, and the history of its use in attacks against City officials, the baseline threat to municipal facilities from this event is assessed to be LOW.

The device may be packaged in a large, padded shipping envelope or small box containing at least 100 grams (TNT equivalent) of explosive material. The device may be initiated through a specific, intended victim action and may contain an electrical initiator. The device may contain enhancements, such as nails, metal ball bearings, or broken glass, intended to increase lethality or injury. Black or smokeless powders have also been used, but this requires a containment vessel and a larger package.

A review of emplaced IEDs on the DHS TRIPwire database reveals only 12 incidents of actual IED devices associated with mail. All of the incidents reported indicate an IED being placed within a mailbox or a suspicious package reported. All of the suspicious packages reported within the time period of August 2014 through July 2015 were determined to be benign/rendered safe.

5.9.2 Outlook

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

The number of actual incidents involving letter bombs over the past 25 years is low and expected to continue at that rate. It is projected that the letter and package bombs may trend toward smaller packaging as the necessary components continue to be miniaturized. For example, greeting cards now provide a power source and a switch in one small package. The limiting factors continue to be smaller initiators (smaller than a standard blasting cap) and the overall size of the main charge.

Undesirable Event	5.10 Explosive Device — Man-Portable				
Definition	An explosive device concealed in a backpack, briefcase or other innocuous container which is capable of being carried by a single operative, and placed outside of a secure area, near an entrance to the facility or carried into a facility by an adversary or an unsuspecting occupant, visitor or courier and left to detonate after the adversary departs.				
Original Assessment	8/1/2017	Revision	1	Date	8/1/2018

5.10.1 Baseline Threat

Based on the generally unrestricted access outside of a secure area, the nature of the attack, availability of materials and instructions, presence of multiple adversary groups who are known to use it as a tactic, disruption of recent plots, and historical frequency of events, including those directed at City facilities, the baseline threat to municipal facilities from this event is assessed to be MEDIUM.

Person-borne improvised explosive devices concealed in item such as a backpack generally target personnel within the lethal blast or fragmentation radius of the device.

5.10.2 Outlook

The use of person-borne IEDs continues to be a frequent occurrence, although targeting of City facilities is infrequent. The use of a man-portable IED placed outside of a secure area at City facility continues to be a likely method of attack, if constructions and evasion of detection occur. Smaller IEDs are easier to construct without being detected by authorities, hence the increase probability of this method being employed above others. Finally, many of the attackers engaging in spree shooting or active shooter scenarios either intended to emplace IEDs or IEDs were discovered at/in their property during the post incident investigation. Facilities with increased target attractiveness feature for Ballistic Attacks should also consider this event as a secondary incident to the attack. Commercial and City facilities were the most prevalent targets according to the data reviewed on DHS TRIPwire.

Undesirable Event	5.11 Arson					
Definition	Deliberately or attempting to set fire in or around a facility or associated grounds and assets.					
Original Assessment	8/1/2017	Revision	1	Date	8/1/2018	

5.11.1 Baseline Threat

Based on the unsophisticated nature of the attack, availability of specific information on planning and executing such an attack, the historical frequency of its use against municipal facilities, and the lack of a demonstrated intent by terrorist organizations to use this tactic against municipal facilities, the baseline threat to City facilities from this event is assessed to be LOW.

There is no history of Arson incidents for City controlled facilities.

5.11.2 Outlook

The potential for eco-terrorists or other like-minded extremists to use arson as an attack method, to include IIDs, makes it likely that this type of attack will continue in the future.

Undesirable Event	5.12 Active Shooter					
Definition	An active shooter is an individual actively engaged in killing or attempting to kill people in a confined and populated area, typically through the use of firearms.					
Original Assessment	8/1/2017	Revision	1	Date	8/1/2018	

5.12.1 Baseline Threat

Based on the availability of firearms, the unsophisticated nature of the attack, the historical frequency of the event specifically against City facilities, as well as an increase in successful and thwarted attacks in the past few years, the baseline threat to City facilities from this event is assessed to be LOW.

Active Shooter attacks continue to steadily increase in frequency since 2000. The gradual increase has resulted in approximately 12 cases per year (with 16 events in 2015). This method of attack remains the most simplistic and capable of producing the highest casualties when employed. A number of international terrorist organizations have encouraged this method through open source publications and social media. Moreover, individuals experiencing high amounts of stress and disconnection with society have employed this method of attack to gain attention.

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

The State of Colorado has had four active shooter incidents within the past five years. The 2012 Aurora shooting, 2013 Arapahoe High School shooting, October 2015 Colorado Springs shooting and the November 2015 Colorado Springs shooting events.

5.12.2 Outlook

Active shooter incidents are typically unsophisticated, require little to no training, and are most often perpetrated by a lone adversary, making them difficult to predict or determine trends. Based on the frequency and success of these types of attacks in recent years, lone adversaries currently present a significant threat to City facilities. It is expected that random acts of violence such as the active shooter scenarios will continue.

Undesirable Event	5.13 Ballistic Attack – Small Arms				
Definition	One or more individuals armed with small arms fire indiscriminately at a facility or in the vicinity of a facility from outside.				
Original Assessment	8/1/2017	Revision	1	Date	8/1/2018

5.13.1 Baseline Threat

Based on the unsophisticated nature of the attack, the historical frequency of the event specifically against City facilities, and well-publicized events in general, the baseline threat to City facilities from this event is assessed to be LOW.

Small arms gunfire may involve the use of weapons categorized as “small arms” or “light weapons;” specifically revolvers, semi-automatic pistols, rifles, shotguns, assault rifles, and light machine guns, among others. Small arms are the weapon of choice in attacks due to their availability and ease of use, transport, and concealment. In an article, published in 2009, local governments were increasingly confronted with the issue, with weapons violations on municipal properties up by 10% percent, while threats against forward facing agencies climbed 11%.

5.13.2 Outlook

Random small arms attacks directed at City facilities are expected to continue at a sporadic, but unpredictable, frequency. Directed attacks are most often perpetrated by lone adversaries. The unpredictable nature of the motivations of lone adversaries makes it difficult to determine what specific factors will make a facility or individual a more attractive target to a lone adversary.

Undesirable Event	5.14 Unauthorized Entry				
Definition	Unauthorized access to a facility or controlled space by forced entry or by stealth.				
Original Assessment	8/1/2017	Revision	1	Date	8/1/2018

5.14.1 Baseline Threat

Based on the unsophisticated nature of the event, nationwide crime statistics, and the frequency of events at City facilities, the baseline threat to City facilities from this event is assessed to be LOW.

In 2015, there were an estimated 1,579,527 burglaries, a decrease of 7.8 percent when compared with 2014 data. The number of burglaries decreased nationally by 27.7 percent when compared with 2011 data and was down 28.0 percent when compared with the 2006 estimate. By subcategory, 57.9 percent of burglaries involved forcible entry, 35.5 percent were unlawful entries, and 6.6 percent were attempted forcible entry. Victims of burglary offenses suffered an estimated \$3.6 billion in property losses in 2015. The average dollar loss per burglary offense was \$2,316. Burglaries of residential properties accounted for 71.6 percent of all burglary offenses.

5.14.2 Outlook

According to the FBI UCR statistics for 2014 and 2015, burglary overall increased 18.9%, (164 compared to 195). The State of Colorado saw an estimated 18,432 burglaries, 6,170 in the region and only 895 locally. Based on the local trend analysis burglaries are expected to increase as the population in the immediate area increases.

Undesirable Event	5.15 Breach of Access Control Point—Covert				
Definition	Use of deceit, coercion, or social engineering to gain access to a controlled space.				
Original Assessment	8/1/2017	Revision	1	Date	8/1/2018

5.15.1 Baseline Threat

The availability of information and sources of manufacturing of false identification cards, and the Historical use of fraudulent IDs as part of a criminal enterprise or for illegal purchases and identity theft, suggests significant opportunity exists to breach an access control point to commit a crime or for other nefarious purposes. Although there have been recent examples of mostly illegal (undocumented) aliens using fraudulent identification in attempts to access various military installations to work construction projects, as well as other individuals using fraudulent military

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

identification in their attempts to gain access, there is no historical basis to suggest they have had any terrorism nexus. Consequently, the baseline threat to City facilities from this event is assessed to be LOW.

Adversaries may use identification, whether fraudulent or legitimate, as a credential in order to obtain access to a facility for illegitimate purposes. Types of identification may include passports, driver’s licenses, and Social Security cards.

5.15.2 Outlook

The implementation of new measures by the City, such as electronic access control, is a significant step forward in preventing the acquisition of fraudulent identification cards. In addition, the more widespread use of electronic means of authentication of access credentials, including biometric identification, makes the creation of fraudulent credentials more challenging. However, criminals and other adversaries continue to adapt and overcome these measures with improved technologies and techniques of their own. This is expected to present a somewhat cyclical trend in the technological effort. In general, though, the advancement in the use of technology may lead to a shift in the focus of adversaries to the use of social engineering techniques to obtain access or steal legitimate credentials and move away from attempts to create fraudulent credentials. In addition, improvements in technology which aid in the prevention of creating fraudulent access badges may cause determined adversaries to resort to overt attempts at breaches.

Undesirable Event	5.16 Disruption of Facility or Security Systems				
Definition	Physically accessing facility or security systems for the purpose of disruption or manipulation of the systems.				
Original Assessment	8/1/2017	Revision	1	Date	8/1/2018

5.16.1 Baseline Threat

Based on the unsophisticated nature of this event and mitigated by the infrequent use against City facilities, the baseline threat to City facilities from this type of event is assessed to be LOW.

Scenario 1: Adversaries gain access to the power supply to several of a building’s CCTV cameras with the intent to disable the cameras.

Scenario 2: Adversary gains access to building’s HVAC control system with the intent to disable building operations.

The disruption of building and security systems has not been an activity on which terrorists focus. Terrorists prefer to engage in major structural sabotage in order to cripple services, transportation systems, or other types of critical infrastructure, rather than just disrupt a building’s operating systems. It is possible, however, that lone adversaries may want to conceal their identity by

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

disabling a facility’s building or security system when committing a crime of theft or burglary or for other nefarious reasons such as pre-operational surveillance. An example of such an event took place in March 2003, when several surveillance cameras at a Kentucky water facility were turned away from their views of a storage tank and facility entrances. Upon investigation, it was determined that an adversary had scaled a fence and accessed the top of a storage tank.

5.16.2 Outlook

Trends show that attacks or plots on structures and facility systems are usually aimed at bridges, tunnels, oil refineries, and maritime ports, indicating that the attackers conducted diligent pre-operational surveillance for extended periods of time. The suspect in the Brooklyn Bridge Plot surveyed the bridge to determine the best location to sever cables with a blowtorch. Multiple terrorist resources stress the importance of continued surveillance before an attack on critical infrastructure.

Undesirable Event	5.17 Chemical/Biological/Radiological (CBR) Release—Internal				
Definition	Intentional release of a CBR agent carried into a facility, including in general interior spaces (lobbies) or into specific rooms or systems (HVAC rooms).				
Original Assessment	8/1/2017	Revision	1	Date	8/1/2018

5.17.1 Baseline Threat

Based on the relative infrequency, and lack of attacks against City facilities to date, the baseline threat to municipal facilities from this event is assessed to be LOW.

A single adversary releases toxic agent (i.e., sarin gas) or a chemical irritant (i.e., pepper spray) by dispersing it in the lobby of a City building.

International terrorist leadership historically has given high priority to CBR attacks to achieve mass casualty goals. Domestic terrorists probably lack the capability to construct and use CBR weapons in mass casualty attacks due to the significant scientific, technical, and logistical hurdles that must be overcome, but could prepare crude materials or obtain toxic industrial chemicals for small scale attacks. Domestic terrorist groups show little interest in a sophisticated CBR capability.

Lone adversaries are more likely to use a CBR weapon to attack within the U.S. than domestic terrorist groups. Since January 2002, only six confirmed domestic incidents involved the attempted acquisition, attempted production, successful production, or actual dissemination of CBR material. Two involved cyanide, and one involved sarin. All cases are known or believed to be linked to lone adversaries with limited capability that operated

5.17.2 Outlook

Toxic industrial chemicals and toxins probably will remain the attack materials of choice for domestic actors seeking to use chemical or biological agents because of their availability and the relative ease of production and/or dissemination.

Undesirable Event	5.18 Chemical/Biological/Radiological (CBR) Release—Mail or Delivery				
Definition	A CBR substance or dispersal device sent to the facility through U.S. Mail or a commercial delivery service, including an unwitting courier.				
Original Assessment	8/1/2017	Revision	1	Date	8/1/2018

5.18.1 Baseline Threat

Despite the continuing interest and intent by certain terrorist organizations in this method of attack, the sophisticated nature and limited literature on creating an effective agent, and the recent lack of history of such attacks against municipal facilities, the baseline threat to City facilities from this event is assessed to be LOW.

5.18.2 Outlook

Ricin and toxic chemicals will probably remain the CBR materials of choice for a mailed package, unless new technologies make it easier to manufacture and disseminate other agents. Domestic terrorists who intend to use chemical or biological materials will likely continue to prefer those that are easily produced or obtained. It is likely that terrorist organization, along with a handful of lone adversaries, will continue to pursue chemical and biological materials, but most domestic terrorist groups will probably continue to have little or no intent or capability to use CBR weapons.

Undesirable Event	5.19 Release of Onsite Hazardous Materials				
Definition	Unauthorized access to hazardous materials stored onsite with the intent of harming personnel or damaging the facility.				
Original Assessment	8/1/2017	Revision	1	Date	8/1/2018

5.19.1 Baseline Threat

Based on the limited locations where hazardous materials are stored at City facilities, the unavailability of information to an adversary, and the lack of historical frequency, the baseline threat to City facilities from this event are assessed to be LOW.

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

5.19.2 Outlook

The storage of large quantities of hazardous materials at City facilities is not a frequent or widely known practice, thus limiting its attractiveness as a target.

Undesirable Event	5.20 Automobile Ramming				
Definition	Driving a vehicle in an attempt to penetrate a facility (e.g., lobby or loading dock) or breach a defined perimeter.				
Original Assessment	8/1/2017	Revision	1	Date	8/1/2017

5.20.1 Baseline Threat

Based on the historical frequency of the event, the baseline threat to City facilities when a vehicle is used as the weapon is assessed to be LOW.

A 4,700-pound pickup or sport utility vehicle (SUV) traveling at accelerating speed attempts to ram into a facility.

The use of a vehicle as a weapon itself is a frequent tactic. The intent may be to cause property damage, injure or kill building occupants, commit suicide, or to simply make a statement by committing the act without regard to the consequences. In these instances, the adversary is usually experiencing an extreme state of emotional duress, discontentment, or dissatisfaction with an immediate situation.

5.20.2 Outlook

It is estimated that ramming attacks where the vehicle is the weapon will continue at an infrequent and unpredictable rate for the foreseeable future.

SAMPLE

THIS PAGE INTERNTIONALLY LEFT BLANK

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

Appendix B - Facility Security Level Process and Site Worksheets

Facility Security Level (FSL) Determinations

The Facility Security Level Determinations for City Facilities direct the user to a set of baseline standards that may be customized to address site-specific conditions. It applies to all facilities whether City-owned or leased, to be constructed, modernized, or purchased. This document defines the criteria and process to be used in determining the FSL of City Facilities, a categorization that then serves as the basis for implementing protective measures under the prescribed security criteria and standards. It is critical that departments and agencies recognize that the security decision process is an integral part of overall facility management and real estate acquisition processes. The security decision process must be fully integrated into the decision-making process to be the most effective.

The initial Facility Security Level (FSL) determination should be made as soon as practical. The FSL determination ranges from a Level I (lowest risk) to Level III (highest risk). The frequency of risk assessments is conducted in accordance with the risk level. The FSL will be reviewed and adjusted, if necessary, as part of each initial and recurring risk assessment. The responsibility for making the final FSL determination rests with the tenant(s) who must devise a risk management strategy and, if possible, fund the appropriate security countermeasures to mitigate the risk:

- For single-tenant facilities owned or leased by the City. The City Manager in coordination with a representative of the tenant directorate will make the FSL determination.
- In multi-tenant facilities owned or leased by the City, the City Manager will coordinate with a representative from each tenant and make the FSL determination.

Facility Security Level Determination Worksheet

The facility security level matrix is comprised of five equally weighted security evaluation factors with corresponding points of 1, 2, or 3 allocated for each factor. The sections that follow provide the criteria to be used in evaluating each factor and assigning points. However, the criteria cannot capture all the circumstances that could be encountered. Thus, the standard includes a sixth factor (intangibles) to allow the assessor to consider other factors unique to the department/agency needs or to the facility.

To use the Facility Security Level (FSL) matrix, each of the factors is examined and a point value assigned based on the provided scoring criteria. The points for all factors are then added together and a primary FSL is identified based on the sum. The assessor may then consider any intangibles that might be associated with the facility. An adjustment to the FSL may be made (and documented accordingly), and a final FSL determined.

Factors	Points			Score
	1	2	3	
Mission Criticality	LOW	MEDIUM	HIGH	
Symbolism	LOW	MEDIUM	HIGH	
Facility Population	< 100	101-250	251 & higher	
Facility Size	Less than 10,000 sq. ft.	10,001-100,000 sq. ft.	Greater than 100,000 sq. ft.	
Threat to Tenant	LOW	MEDIUM	HIGH	
Facility Security Level	I (Low) 5-7 Points	II (Medium) 8-12 Points	III (High) 13-15 Points	
Preliminary FSL				
Intangible Adjustments				
Final FSL				

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

Mission Criticality

The mission criticality score is based on the criticality of the missions carried out by tenants in the facility (not by the tenant agencies overall). In a multi-tenant or mixed-multi-tenant facility, the highest rating for any tenant in the facility should be used for this factor.

Value	Points	Criteria
High	3	Houses personnel or specialized equipment necessary to detect or respond to unique public health incidents. Houses material or information that, if compromised, could cause a significant loss of life, including production quantities of chemicals, biohazards, explosives, weapons, etc. Irreplaceable material or information central to the daily conduct of the City. Designated as a shelter in the event of an emergency incident.
Medium	2	City-wide service or regulatory operations. Single office Agency.
Low	1	Administrative services. Recreational Services

Symbolism

The symbolism of the facility is based on both its attractiveness as a target and the consequences of an event. The symbolic value is first based on external appearances or well-known/publicized operations within the facility that indicate it is a City facility. Domestic radicals may seek to make a statement against state/City controlled, taxation, policies, or regulation.

Value	Points	Criteria
High	3	A nationally significant historical event has occurred at the facility. Other prominent symbols of Government or authority. Well-known, regional Government facility.
Medium	2	Readily identified as a state/City facility based external features. Readily identified as a state/City facility based on the nature of public contact or other operations (even without external features). A facility that may be symbolic to single-interest radicals.

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

Low	1	No external features or public contact readily identifying it as a state/City facility.
-----	---	---

Facility Population

The facility population factor is based on the peak total number of personnel in City space, including employees, onsite contract employees, and visitors. This number should not include such transient influxes in population as an occasional conference (or similar event) unless the facility is intended for use in such a manner (such as a conference center) and the population is part of normal business. Transient shifts in the population such as the occasional conference should be addressed by contingency security measures. The number of daily visitors should be determined using the best metrics available to ensure the most accurate population.

Value	Points	Criteria
High	3	Over 250
Medium	2	100 to 250
Low	1	Less than 100

Facility Size

The facility size factor is based on the square footage of all City-occupied space in the facility. Including cases where an agency with real property authority controls some other amount of space in the facility. If the entire facility or entire floors are occupied, gross square footage should be used (length x width): If only portions of floors are occupied in a multi-tenant facility, assignable or rentable square footage should be used. Size may be directly or indirectly proportional to the facility population. An office facility with a large population will generally have a correspondingly large amount of floor space; however, a large warehouse may have a very small population.

Value	Points	Criteria
High	3	Greater than 100,000 square feet
Medium	2	10, 000 to 100, 000 square feet
Low	1	Less than 10,000 square feet

Threat to Tenant Agency

The facility should be viewed in terms of whether the nature of public contact required in or resulting from the conduct of business is adversarial, or whether there is a history of adversarial acts committed at the facility, against facility tenants, or against the tenant agencies elsewhere. The highest score applicable to any tenant in a multi-tenant facility will be considered when determining the FSL even though it may be possible to limit the implementation of countermeasures for that threat to a specific tenant’s space or part of the facility.

Value	Points	Criteria
High	3	Tenant mission and interaction with certain segments of the public is adversarial in nature. Tenant mission is controversial in nature and routinely draws the attention of organized protest groups. Located in a high-crime area. Significant history of violence directed at or occurring in the facility. More than 10 incidents per year requiring law enforcement/security response for unruly or threatening persons on-site.
Medium	2	Public contact is occasionally adversarial based on the nature of the business conducted at the facility. History of demonstrations against at the facility. Located in a moderate-crime area. History of violence directed at tenant’s agencies (not at the facility).
Low	1	Generally little-to-no public contact. No history of demonstrations at the facility. Located in a low-crime area. No history of violence directed at the facility or the occupants.

This report is confidential; the disclosure of its contents would be contrary to the public interest.
 This report is therefore unavailable for public inspection.

a. **Municipal Building Worksheet**

Facility Security Level Determination Worksheet				
<p>The facility security level matrix is comprised of five equally weighted security evaluation factors with corresponding points of 1, 2, or 3 allocated for each factor. The sections that follow provide the criteria to be used in evaluating each factor and assigning points. However, the criteria cannot capture all the circumstances that could be encountered. Thus, the standard includes a sixth factor (intangibles) to allow the assessor to consider other factors unique to the department/agency needs or to the facility.</p> <p>To use the Facility Security Level (FSL) matrix, each of the factors is examined and a point value assigned based on the provided scoring criteria. The points for all factors are then added together and a primary FSL is identified based on the sum. The assessor may then consider any intangibles that might be associated with the facility. An adjustment to the FSL may be made (and documented accordingly), and a final FSL determined.</p>				
Factors	Points			Score
	1	2	3	
Mission Criticality	LOW	MEDIUM	HIGH	3
Symbolism	LOW	MEDIUM	HIGH	3
Facility Population	< 100	101-250	251 & higher	3
Facility Size	Less than 10,000 sq. ft.	10,001- 100,000 sq. ft.	Greater than 100,000 sq. ft.	2
Threat to Tenant	LOW	MEDIUM	HIGH	2
Facility Security Level	I (Low) 5-7 Points	II (Medium) 8-12 Points	III (High) 13-15 Points	13
Preliminary FSL				3
Intangible Adjustments				None
Final FSL				3

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

b. Recreation Building Worksheet

Facility Security Level Determination Worksheet				
<p>The facility security level matrix is comprised of five equally weighted security evaluation factors with corresponding points of 1, 2, or 3 allocated for each factor. The sections that follow provide the criteria to be used in evaluating each factor and assigning points. However, the criteria cannot capture all the circumstances that could be encountered. Thus, the standard includes a sixth factor (intangibles) to allow the assessor to consider other factors unique to the department/agency needs or to the facility.</p> <p>To use the Facility Security Level (FSL) matrix, each of the factors is examined and a point value assigned based on the provided scoring criteria. The points for all factors are then added together and a primary FSL is identified based on the sum. The assessor may then consider any intangibles that might be associated with the facility. An adjustment to the FSL may be made (and documented accordingly), and a final FSL determined.</p>				
Factors	Points			Score
	1	2	3	
Mission Criticality	LOW	MEDIUM	HIGH	1
Symbolism	LOW	MEDIUM	HIGH	2
Facility Population	< 100	101-250	251 & higher	3
Facility Size	Less than 10,000 sq. ft.	10,001- 100,000 sq. ft.	Greater than 100,000 sq. ft.	2
Threat to Tenant	LOW	MEDIUM	HIGH	2
Facility Security Level	I (Low) 5-7 Points	II (Medium) 8-12 Points	III (High) 13-15 Points	10
Preliminary FSL				2
Intangible Adjustments				None
Final FSL				2

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

c. Adult Center Worksheet

Facility Security Level Determination Worksheet				
<p>The facility security level matrix is comprised of five equally weighted security evaluation factors with corresponding points of 1, 2, or 3 allocated for each factor. The sections that follow provide the criteria to be used in evaluating each factor and assigning points. However, the criteria cannot capture all the circumstances that could be encountered. Thus, the standard includes a sixth factor (intangibles) to allow the assessor to consider other factors unique to the department/agency needs or to the facility.</p> <p>To use the Facility Security Level (FSL) matrix, each of the factors is examined and a point value assigned based on the provided scoring criteria. The points for all factors are then added together and a primary FSL is identified based on the sum. The assessor may then consider any intangibles that might be associated with the facility. An adjustment to the FSL may be made (and documented accordingly), and a final FSL determined.</p>				
Factors	Points			Score
	1	2	3	
Mission Criticality	LOW	MEDIUM	HIGH	1
Symbolism	LOW	MEDIUM	HIGH	2
Facility Population	< 100	101-250	251 & higher	2
Facility Size	Less than 10,000 sq. ft.	10,001- 100,000 sq. ft.	Greater than 100,000 sq. ft.	2
Threat to Tenant	LOW	MEDIUM	HIGH	2
Facility Security Level	I (Low) 5-7 Points	II (Medium) 8-12 Points	III (High) 13-15 Points	9
Preliminary FSL				2
Intangible Adjustments				None
Final FSL				2

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

Appendix C – Baseline Physical Security Standards

Details of Security Measures

Effective deployment of countermeasures requires a full understanding of the recommended Security measure. Accordingly, the tables below give details of selected security measures identified in the security industry. Criteria are grouped according to **site, structure, facility entrances, interior, security systems, and operations and administration**. Additional details are provided to convey the full meaning and scope of those baseline security measures whose title and brief description alone are not sufficient. For those measures for which additional detail is not provided, the baseline description is considered sufficient.

Baseline Physical Security Criteria

SITE SECURITY CRITERIA

Criteria No.	Security Criteria	Level I Low	Level II Medium	Level III High
1	Identification as City Facility	No special measures required	No special measures required	Signage identifying a facility as a City facility should only be posted when necessary to achieve the mission of the tenants, or when the facility is readily identified or well known as a City facility based on the nature of public contact or other operations.
2	Landscaping	Minimize areas of concealment in and around facilities	Minimize areas of concealment in and around facilities.	Restrict landscaping from obstructing the view of the security guards and CCTV cameras, or interfering with lighting or IDS.

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

CONFIDENTIAL

Criteria No.	Security Criteria	Level I Low	Level II Medium	Level III High
3	Pedestrian Access to Site	No special measures required	No special measures required	In a campus environment, install fences, landscaping, or other barriers to channel pedestrians to authorized areas or entrances.
4	Vehicle Access Points	No special measures required	No special measures required	Limit the number of vehicle access points.
5	Site Lighting	Install exterior lighting at entrances and exits.	Install exterior lighting at entrances, exits, parking lots, garages, and walkways from parking areas to entrances.	Install exterior lighting at entrances, exits, parking lots, garages, and walkways from parking areas to entrances
6	Restricted Areas	No special measurements required.	Provide fences, walls, gates, or other barriers to prevent unauthorized access to restricted areas.	Provide fences, walls, gates, or other barriers to prevent unauthorized access and observation to restricted areas and monitor with CCTV or guard patrol.
7	Signage for Sensitive Areas	No special measurements required.	Prohibit signs that identify sensitive areas, unless required by other standards/codes.	Prohibit signs that identify sensitive areas, unless required by other standards/codes.
8	Control of Parking	No special measurements required.	No special measurements required.	Control vehicle access to underground/in-building parking.

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

CONFIDENTIAL

Criteria No.	Security Criteria	Level I Low	Level II Medium	Level III High
9	Authorized Parking	No special measurements required.	Limit parking to employee vehicles, authorized visitor vehicles, approved City vehicles, and other authorized parkers	Limit parking to employee vehicles, authorized visitor vehicles, approved City vehicles, and other authorizes parkers. Screen visitors and approved City vehicles during high-risk periods.
10	Vehicle Access to Control Parking	No special measures required	Designate employee and visitor parking areas.	Use vehicle gates to limit access to authorized vehicles only.
11	Vehicles Barriers	No special measures required	No special measures required	Provide vehicle barriers to protect pedestrian entrances from penetration by a vehicle meeting the DBT.
12	Vehicle Screening	No special measures required	No special measures required	Screen visitor vehicles before entry into the controlled parking area. Randomly screen employee, approved City, and contractor vehicles during heightened security alerts.
13	Pedestrian Access to Controlled Parking	No special measures required	Minimize areas of concealment in and around parking areas.	Provide barriers to restrict pedestrian access into parking

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

CONFIDENTIAL

Criteria No.	Security Criteria	Level I Low	Level II Medium	Level III High
	Areas			areas to authorized entry points.
14	Hazardous Materials Storage	No special measures required	Locate HAZMAT in a restricted area away from the loading dock, entrances, and uncontrolled parking.	Locate HAZMAT in a restricted area away from the loading dock, entrances, and uncontrolled parking.
15	Receptacle and Container Replacement	No special measures required	Position trash containers, mailboxes, vending machines, or other fixtures and features that could conceal devices away from building entrances.	Position trash containers, mailboxes, vending machines, or other fixtures and features that could conceal devices away from building entrances.

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

STRUCTURE SECURITY CRITERIA

Criteria No.	Security Criteria	Level I Low	Level II Medium	Level III High
16	Blast Resistance Window	No special measures required	No special measures required	Use acceptable fragment retention film, or acceptable glazing systems to reduce the glass fragmentation hazard
17	Blast Resistance Façade and Structure	No special measures required	No special measures required	Use a combination of setback, site planning, façade hardening, and structure measures to provide a medium level of façade protection.
18	Blast Resistance Progressive Collapse	No special measures required	No special measures required	For buildings over three stories, use a combination, site planning, façade hardening, and structure measures to prevent progressive collapse from the DBT or the loss of any single exterior column or load bearing wall whichever is lower.
19	Blast Resistance Under Building Parking	No special measures required	Use construction materials which have inherent ductility and which are better able to respond to load reversal (e.g., cast in place reinforcement	Implement architectural or structural features, or other positive countermeasures (e.g., vehicle screening), that deny contact with exposed primary vertical load members in these

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

CONFIDENTIAL

Criteria No.	Security Criteria	Level I Low	Level II Medium	Level III High
			concrete column construction)	areas. A minimum standoff of at least 150 mm (6 inches) from these members is required.
20	Burglary Resistance of Windows	Lock all operable ground floor windows.	Lock all operable ground floor windows.	No operable windows on ground floor level.
21	Walls and Non-window Openings	No special measures required	Protect non-window opening such as Mechanical vents and exposed plenums to resist forcible entry.	Protect non-window opening such as Mechanical vents and exposed plenums to resist forcible entry.
22	Windows in Critical Areas – Ballistic Protection	No special measures required	Provide blinds, curtains, or other window treatments in critical areas that can be used to prevent visual observation into critical areas when conditions warrant.	Prevent observation from the exterior into critical exterior offices.
23	Protection of Air Intake	Provide emergency shutdown, Shelter in Place (SIP), and evacuation procedures.	Provide emergency shutdown, Shelter in Place (SIP), and evacuation procedures and secure accessible air intake grills	Provide emergency shutdown, Shelter in Place (SIP), and evacuation procedures and protect accessible air intake with fencing. Monitor with CCTV or guard patrols.

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

CONFIDENTIAL

Criteria No.	Security Criteria	Level I Low	Level II Medium	Level III High
			from tampering or removal.	
24	Isolated Ventilation Systems	No special measures required	Provide separate isolated HVAC systems in lobbies, loading docks, mailrooms, and other locations susceptible to CBR attack that are isolated from other building areas.	Provide separate isolated HVAC systems in lobbies, loading docks, mailrooms, and other locations susceptible to CBR attack that are isolated from other building areas. Ensure that the envelope of the isolated loading dock and mailroom are full-height construction and are sealed to the floor roof or ceiling above.
25	HVAC Control	No special measures required	Develop written procedures of the emergency shutdown or exhaust of air handling systems.	Install a one-step shut-off and exhaust system for air handlers. Control movement of elevators, and close applicable doors and dampers to seal the building. Provide an emergency response module to the building energy-management system to switch the system to a prescribed emergency response mode.
26	Biological Filtration General Building	No special measures required	Use a Minimum Efficiency Reporting (MERV) 10	Use a Minimum Efficiency Reporting (MERV) 13 particulate filter on

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

CONFIDENTIAL

Criteria No.	Security Criteria	Level I Low	Level II Medium	Level III High
			particulate filter on all exterior air handling units (AHUs).	all exterior air handling units (AHUs). Including the supply air stream for recirculating AHUs.
27	Biological Filters Lobbies and Mailrooms	No special measures required	Use a Minimum Efficiency Reporting (MERV) 13 particulate filter on all exterior air handling units (AHUs) in mailrooms and lobbies.	Use a Minimum Efficiency Reporting (MERV) 13 particulate filter on all exterior air handling units (AHUs). Including the supply air stream for recirculating AHUs in mailrooms and lobbies.
28	Security of Ventilation Equipment and Controls	No special measures required	Protect the system controls from unauthorized access.	Provide IDS coverage of ventilation equipment and control rooms.
29	Location of Utilities and Feeders	No special measures required	No special measures required	Locate utility systems at least 25 feet away from loading docks, entrances, and uncontrolled parking, or implement standoff, hardening and venting methods to protect utilities from the DBT at these locations.
30	Separation of Emergency and Normal Power Distribution	No special measures required	No special measures required	Install emergency and normal power systems (including electrical panel, conduits, and switchgear) at least 25 feet apart.

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

Criteria No.	Security Criteria	Level I Low	Level II Medium	Level III High
31	Emergency Generator Protection	No special measures required	If an emergency generator is used, secure it against unauthorized access.	If an emergency generator is used, secure it against unauthorized access, and locate the emergency generator and fuel tank at least 25 feet away from loading docks, entrances, parking, or implement standoff, hardening, and venting, methods to protect utilities from the DBT at these locations.
32	Protection of Water Supply	No special measures required	Secure handles, control mechanism, and service connection at on-site publicly-accessible locations with locks or other anti-tamper devices.	Secure handles, control mechanism, and service connection at on-site publicly-accessible locations with locks or other anti-tamper devices.

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

FACILITY ENTRANCE SECURITY CRITERIA

Criteria No.	Security Criteria	Level I Low	Level II Medium	Level III High
33	Badge Identification (ID) System	No special measures required	Require agency photo ID that is worn and visible always when in City controlled space.	Require agency photo ID that is worn and visible always when in City controlled space.
34	Regulatory Signage	Post necessary regulatory, statutory, and/or site specific signage.	Post necessary regulatory, statutory, and/or site specific signage.	Post necessary regulatory, statutory, and/or site specific signage.
35	Employee Access Control	Issue employee keys for access	Provide a means to secure employee entrance doors. Require ID badge presentation to guards for visual and physical inspection before entry.	Provide a means to secure employee entrance doors. Require ID badge presentation to guards for visual and physical inspection before entry.
36	Visitors Access Control	Entrances are open to the public during business hours. After hours, visitor entrances are secured and have means to verify the identity of persons requesting	Entrances are open to the public during business hours. After hours, visitor entrances are secured and have means to verify the identity of persons requesting	Require visitors to nonpublic areas be sponsored by a tenant and either approved for unescorted access or escorted at all times.

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

CONFIDENTIAL

Criteria No.	Security Criteria	Level I Low	Level II Medium	Level III High
		access prior to allowing entry into the facility.	access prior to allowing entry into the facility.	
37	Occupant Screening	No special measures required.	No special measures required.	Use X-ray and magnetometer to screen all occupants and their property that do not possess and acceptable ID for access to the facility.
38	Visitor Screening	No special measures required.	No special measures required.	Screen all visitors and their property using X-ray and magnetometer.
39	Lobby Queuing	No special measures required.	No special measures required.	Minimize queuing caused by screening, visitor processing, and access control system throughput.
40	After Hours Access Control	No special measures required	No special measures required	Require all employees, contractors, and visitors to sign in and sign out electronically, or on a building after hours register.
41	Limit Building Entry Points	No special measures required	No special measures required	Limit the number of building entry points to the fewest number practical.
42	Entrance Co-location	No special measures required	Create separate flow patterns for	Create separate entrances for employee and

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

CONFIDENTIAL

Criteria No.	Security Criteria	Level I Low	Level II Medium	Level III High
			employee and visitors at entrances.	visitors.
43	Perimeter Doors and Door Locks	Secure perimeter doors with high-security mechanical locks.	Secure perimeter doors with high-security mechanical locks.	Secure doors with nonremovable hinges and high-security mechanical or electronic locks.
44	Control of Keys and Access Media	Implement a formal key control and access media program.	Implement a formal key control and access media program.	Implement a formal key control and access media program.
45	Employee Convenience Doors	No special requirements required	No special requirements required	Provide electronic access control from employee entry doors without a guard post (including after hour access) in conjunction with CCTV coverage.
46	Emergency Exit Doors	Secure emergency exit doors using an automatic door closer and exit hardware that are compliance with applicable life safety codes and standards.	Secure emergency exit doors using an automatic door closer and exit hardware that are compliance with applicable life safety codes and standards.	Secure emergency exit doors using an automatic door closer and exit hardware that are compliance with applicable life safety codes and standards.
47	Delayed Egress	No special requirements required	No special requirements required	Use delayed egress hardware at emergency exits from critical or sensitive areas, if fire code allows.

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

INTERIOR SECURITY CRITERIA

Criteria No.	Security Criteria	Level I Low	Level II Medium	Level III High
48	Space Planning	No special measures required	Locate critical systems and areas at least 25 feet away from loading docks, entrances, mailrooms, personnel and packaging screening locations, and uncontrolled parking, or implement standoff, hardening, and venting methods to protect critical areas from the DBT at these locations.	Locate critical systems and areas at least 25 feet away from loading docks, entrances, mailrooms, personnel and packaging screening locations, and uncontrolled parking, or implement standoff, hardening, and venting methods to protect critical areas from the DBT at these locations.
49	Access to Nonpublic Areas	Use signage to designate nonpublic areas and establish procedures to prevent unauthorized access.	Use signage, stanchions, counters, furniture, knee walls, etc., to establish physical boundaries to control access to nonpublic areas.	Use signage, walls, IDS, and electronic access control and/or security guards to establish physical boundaries to control access to nonpublic areas.
50	Security of Critical Areas	Lock doors to critical areas and establish procedures to limit access into critical areas to authorized personnel	Install electronic access control and IDS to control and monitor access to critical areas.	Install electronic access control and IDS to control and monitor access to critical areas.

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

Criteria No.	Security Criteria	Level I Low	Level II Medium	Level III High
		only.		
51	Building Systems and Roof Access	Secure utility, mechanical, electrical, and telecom rooms, and access to interior space from the roof with high-security locks.	Secure utility, mechanical, electrical, and telecom rooms, and access to interior space from the roof with locks and IDS.	Secure utility, mechanical, electrical, and telecom rooms and access to interior space from the roof using electronic access control and IDS.
52	Public Accessible Restrooms	Control access to public restrooms.	Screen the public before accessing restrooms.	Screen the public before accessing restrooms.
53	Publicly Accessible Retail and Mixed Use Space	Accommodate publicly accessible retail and mixed uses through such means as a separate entryway.	Accommodate publicly accessible retail and mixed uses through such means as a separate entryway.	Accommodate publicly accessible retail and mixed uses through such means as controlling access, screening, and guards.
54	Blast Resistance Interior Public Space	Use construction materials which have inherent ductility and which are better able to respond to load reversal (e.g., cast in place reinforced concrete column construction).	Implement architectural or structural features or other positive countermeasures that deny contact with exposed primary vertical load members in these areas. A minimum standoff of at least 100 mm (4 inches) is required.	Use hardening and venting methods to prevent progressive collapse and limit air-blast injuries in adjacent areas from the DBT in an area accessible to unscreened persons. Significant structural damage to the walls, ceilings, and floors of the public area may occur, however, the

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

Criteria No.	Security Criteria	Level I Low	Level II Medium	Level III High
				adjacent areas should not experience severe damage or collapse.
55	Blast Resistance Mail Screening and Receiving Locations	No special measures required	Use construction materials in the mail screening and receiving areas which have inherent ductility and which are better able to respond to load reversal (e.g., cast in place reinforced concrete column construction).	Use hardening and venting methods to prevent progressive collapse and limit air blast injuries in adjacent areas from the DBT in a mail screening or receiving areas. Significant structure damage to the walls, ceilings, and floors, of the mailroom/receiving area, may occur. However, the adjacent area should not experience severe damage or collapse.
56	Interior Windows	No special measures required.	No special measures required.	Provide tempered or high-strength glass.

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

SECURITY SYSTEMS CRITERIA

Criteria No.	Security Criteria	Level I Low	Level II Medium	Level III High
57	CCTV Coverage	No special measures required	Provide CCTV coverage of screening checkpoints, pedestrian and vehicle entrances, exits, loading docks, and lobbies.	Provide CCTV coverage of screening checkpoints, exits, loading docks, lobbies, facility perimeter, parking areas, sensitive interior areas, pedestrian and vehicle entrances, and other potential access points.
58	CCTV Monitoring and Recording	No special measures required	Record CCTV views using time-lapse video recording.	Record CCTV views using time-lapse video recording and digital image storage.
59	Security Control Center	No special measures required	No special measures required	Provide onsite central security control center, staffed during operating hours.
60	CCTV Surveillance Advisory	Post signage advising of CCTV surveillance when used.	Post signage advising of CCTV surveillance when used.	Post signage advising of CCTV surveillance when used.
61	Intrusion Detection System (IDS) Coverage	Provide IDS on perimeter entrance and exit doors, and all ground floor windows.	Provide IDS on perimeter entrance and exit doors, and all ground floor windows.	Provide IDS on perimeter entrance and exit doors, and all windows within 16 feet of the ground or other access

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

Criteria No.	Security Criteria	Level I Low	Level II Medium	Level III High
				point.
62	Intrusion Detection System (IDS) Monitoring	Monitor at a central station (onsite or offsite) with notification to building manager of designated tenant POC during operating hours and law enforcement or security responders after operating hours.	Monitor at a central station (onsite or offsite) with notification to building manager of designated tenant POC during operating hours and law enforcement or security responders after operating hours.	Monitor at a central station (onsite or offsite) with notification to building manager of designated tenant POC during operating hours and law enforcement or security responders after operating hours.
63	Duress Alarm or Assistance Stations	Implement duress procedures for emergency situations.	Provide duress buttons or call buttons at guard posts and sensitive public contact areas.	Provide duress buttons or call buttons at guard posts, sensitive public contact areas, garages, and other areas that are identified as high-risk locations.
64	Security System Integrity	Secure alarm and physical access control panels, CCTV components, controllers, and cabling	Secure alarm and physical access control panels, CCTV components, controllers, and cabling against unauthorized	Secure alarm and physical access control panels, CCTV components, controllers, and cabling against unauthorized

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

Criteria No.	Security Criteria	Level I Low	Level II Medium	Level III High
		against unauthorized access	access	access.
65	Security Communications	No special measures required.	Provide a centralized radio network for guard-force personnel.	Provide a centralized radio network for guard-force personnel.
66	Building Communication System	No special measures required.	Provide a communication system for security and emergency announcements.	Provide a communication system for security and emergency announcements.
67	Emergency Power for Security Systems	No special measures required.	Provide uninterrupted emergency power to essential electronic security systems for a minimum of four hours.	Provide uninterrupted emergency power to essential electronic security systems for a minimum of four hours.
68	Security System Testing	Conduct security system performance testing annually	Conduct security system performance testing annually.	Conduct security system performance testing semiannually.
69	Security System Maintenance	Implement a preventative maintenance program for all security systems. Any critical component that becomes inoperable must be	Implement a preventative maintenance program for all security systems. Any critical component that becomes inoperable must be replaced or repaired within	Implement a preventative maintenance program for all security systems. Any critical component that becomes inoperable must be replaced or repaired within

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

CONFIDENTIAL

Criteria No.	Security Criteria	Level I Low	Level II Medium	Level III High
		replaced or repaired within ten business days.	five business days.	24 hours.

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

SECURITY OPERATIONS AND ADMINISTRATION CRITERIA

Criteria No.	Security Criteria	Level I Low	Level II Medium	Level III High
70	Designated Official (DO)	Identify the DO who is responsible for security, safety, and emergency management in the facility.	Identify the DO who is responsible for security, safety, and emergency management in the facility.	Identify the DO who is responsible for security, safety, and emergency management in the facility.
71	Facility Security Committee (FSC)	Established an FSC that is chaired by the DO (or designee) to provide oversight of security, life-safety, and emergency procedures.	Established an FSC that is chaired by the DO (or designee) to provide oversight of security, life-safety, and emergency procedures.	Established an FSC that is chaired by the DO (or designee) to provide oversight of security, life-safety, and emergency procedures.
72	Security Operations Manager	No special measures required	Provide a City security manager with oversight responsibilities for guards and other physical security operations who is onsite at least weekly	Provide a City security manager with oversight responsibilities for guards and other physical security operations who is onsite at least each workday
73	Guard Fixed Post-Exterior	No special measures required.	No special measures required.	Provide fixed guard posts to challenge and identify approaching persons prior to entry into the building during heighten risk periods.

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

CONFIDENTIAL

Criteria No.	Security Criteria	Level I Low	Level II Medium	Level III High
74	Guard Fixed Posts-Screening Checkpoints	No special measures Required.	Provide armed guards at all screening checkpoints.	Provide armed guards at all screening checkpoints.
75	Guard Patrols	No special measures Required.	No special measures Required.	Establish hourly interior and exterior roving armed guard patrols during normal business hours.
76	Guard Response	No special measures Required.	Develop plans for onsite security guard response to alarms and incidents.	Develop plans for onsite security guard response to alarms and incidents.
77	Facility Security Plan	Develop a written facility security plan that identifies security responsibilities, emergency contacts, response procedures for incidents, and contingency plans for temporary upgrades.	Develop a written facility security plan that identifies security responsibilities, emergency contacts, response procedures for incidents, and contingency plans for temporary upgrades.	Develop a written facility security plan that identifies security responsibilities, emergency contacts, response procedures for incidents, and contingency plans for temporary upgrades.
78	Occupant Emergency Plan (OEP)	Develop, publish, and maintain an OEP, and conduct annual training /exercises.	Develop, publish, and maintain an OEP, and conduct annual training/exercises.	Develop, publish, and maintain an OEP, and conduct annual training /exercises.

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

CONFIDENTIAL

Criteria No.	Security Criteria	Level I Low	Level II Medium	Level III High
79	Availability of Emergency Plans and Documents	Ensure ready availability of emergency plans and associated documents in the event of an emergency.	Ensure ready availability of emergency plans and associated documents in the event of an emergency.	Ensure ready availability of emergency plans and associated documents in the event of an emergency.
80	Protection of Construction Information	No special measures required.	Limit access to construction documents to those persons with an established need-to-know.	Limit access to construction documents to those persons with an established need-to-know.
81	Security During Construction and Renovation	No special measures required.	Develop and implement a Construction Security Plan.	Develop and implement a Construction Security Plan.
82	Mail /Package Handling and Other Deliveries	Follow City Safe Mail Handling Procedures.	Inspect all mail/packages and deliveries visually prior to distribution throughout the facility.	Screen all mail and packages using X-ray at a loading dock, if present or at an existing screening location if there is no loading dock. Physically inspect items that cannot be passed through screening equipment.
83	Security Awareness Training	Provide all employees with annual security awareness training.	Provide all employees with annual security awareness training.	Provide all employees with annual security awareness training.

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

Appendix D – Detailed Mitigation Strategies (including rough order of magnitude cost estimates)

Our recommendations are based on the principles of Deter, Detect, Delay, Assess, Respond, Neutralize and Recover.

- **Deter**-The measures designed to present a hardened appearance and discourage potential “bad actors” from attacking a facility.
- **Detect**-The measures designed to provide an alert to the monitoring station of a potential undesirable event.
- **Delay**-The measures designed to harden a facility and slow the progress of a potential undesirable event.
- **Assess**-The measures designed to assist the monitoring station in identifying the potential threat and determine an appropriate response.
- **Respond**-Respond-The measures designed to allow the monitoring station to dispatch the appropriate response. This is a two-tiered process. On the first tier emergency responders (guards, law enforcement, etc.) are dispatched to intervene with potential bad actors. On the second tier power system operators, dispatch crews reconfigure the power system to minimize the impact on the grid.
- **Neutralize**-The measures designed to assist security responders in apprehending/removing perpetrators and the Control Center in removing a facility from the transmission network.
- **Recover**-The measures designed to assist in restoring the facility to normal operations.

These principles are depicted in Figure D.1 below.

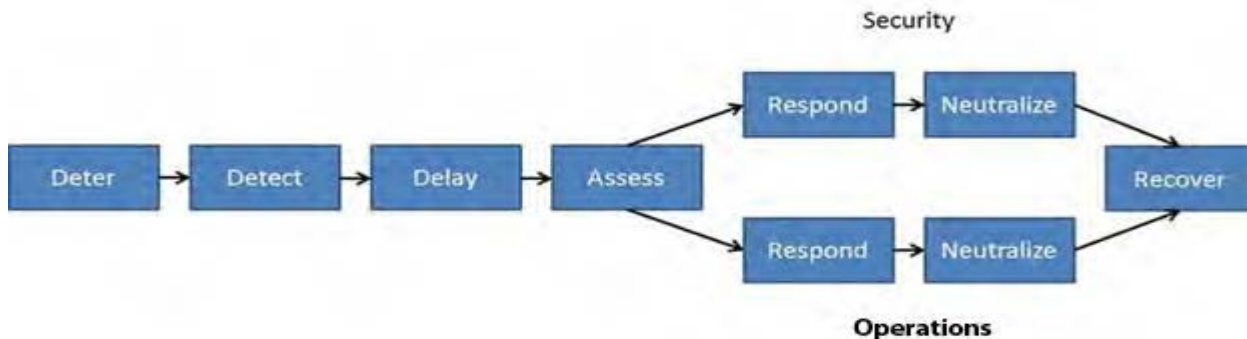


Figure D.1 – The Response Process

Our ROM cost estimates are prepared using RSMeans Online to find reliable cost data on construction materials, equipment, and labor. Construction professionals from all corners of the industry use RSMeans Online to build complete estimates, find and validate construction costs, compare local costs against national averages, or get quick, conceptual estimates for a variety of building types. RSMeans continues to grow and update its construction cost database of over 75,000 unit prices, 25,000 building assemblies and 42,000 facilities repair and remodeling costs covering every category of construction. The cost estimates are only for the associated tasks and do not include any additional surcharges such as service call fees or travel costs.

This report is confidential; the disclosure of its contents would be contrary to the public interest.

This report is therefore unavailable for public inspection.

6.1. Citywide Recommendations

1. The city does not have a single point of contact to manage day-to-day security requirements and program for the City. Create a *Director of Security* position to manage improvements and maintain acceptable security standards for the city. Estimated Cost: \$76,087-\$121,000 annually.
2. Employees do not wear City ID above their waist while on City property or while conducting City business as required. Management should conduct on the spot corrections of employees not properly displaying their City ID. Estimated Cost: None
3. There is a lack of standardized security-related City Wide Emergency Operating Procedures (EOP), and Security Policies. At a minimum create an Emergency Action Plan (standardized), Security Management Plan to include incident reports, Emergency Notification Plan, Access Management Policy (including standardized access request forms and key control), City-wide money-handling policy to include (pick-up/deposit procedures/cash collected and counted in safe room/requirements that safe be secured at all time when not in use), CCTV use policy and Security Equipment Specifications & Installation Standards. Estimated Cost: None
4. The City currently utilizes employee and their personal automobiles for the pickup and transportation of monetary instruments from the city facilities. Pickup and transportation of monetary instruments from city facilities should be conducted in City owned vehicles or establish a third party armored car service. Estimated Cost: TBD
5. The City lacks an operational mass notification system. Program the existing VoIP phone system to serve as the mass notification system. Provide training to appropriate staff on its use and operation. Estimated Cost: \$10,500 one time.
6. The City does not have a city-wide incident reporting system. Purchase and customize a city-wide standardized network-based centralized incident reporting system to report all incidents to the city manager. Estimated Cost: \$5,500 one time
7. The city has not established a standardized security awareness training program for employees and full-time contractors. Establish a standardized security awareness training program, with mandatory city-wide training every 1.5 years and within 90 days for all new hire employees. Estimated Cost: None
8. The current IP cameras log utilizes the factory default password. Immediately change all default passwords. Estimated Cost: None

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

6.2. Municipal Building Recommendations:

1. Administrative offices and city employees have limited security from a violent visitor.
 - a) Establish a screening station at the west public vestibule. Estimated cost: \$45,000.
 - b) Provide two-armed guard to staff the screening station whenever the building is open to the public. Estimated Cost \$135,000 annually.
 - c) Install barrier walls and glass at reception and a new door with card-reader access to prevent unauthorized access to employee workspace. Estimated Cost: \$32,160
 - d) Create separate “Cashier” windows in lobby for all public/cash/check transactions & distribution of permits (pay-&-go). Estimated Cost: \$25,360
 - e) Install call-box on exterior of main lobby entry (for after-hours call to Police Department). Estimated Cost: \$2,653 one time.

2. Several departments conduct meetings with the public in the immediate employee work area which could possibly become confrontational. Utilize the existing “Lobby Conference Room” for meetings with the public. Estimated Cost: None

3. The current safe used to secure monetary fund’s overnight and is not heavy enough to prevent removal. Additionally the safe remains open during operational hours in an employee’s office.
 - a) Purchase a new high-security safe with electronic keypad with multi-user and auditable capability that is properly secured to the floor to properly secure funds. Estimated Cost: 3,842
 - b) Create a separate safe/money-count room. Estimated Cost: \$20,276
 - c) Install card in/card out readers on both entry doors to the safe/money-count room. Estimated Cost: \$6,760
 - d) Install a CCTV camera in the safe/money-count room for observation of access to the safe as well as funds accountability transactions. Estimated Cost: \$3,272

4. Management is not notified of duress alarm activations and there is no written duress procedures established.
 - a) Create a written duress button protocol and communicate to all staff. Estimated Cost: None
 - b) Create a dual-duress notification system for notification of management of incidents at the proposed reception window and new cashier window. Estimate Cost: \$1,530
 - c) Install a duress system in the new safe/money-count room. Estimate Cost: \$1,872

5. The current configuration of the City Council Chambers does not provide adequate security or protection for staff and visitors.
 - a) Move staff desk to stage-left of room adjacent city clerk and install a half wall around the desk to prevent public access. Estimated Cost: \$3,500
 - b) Relocate lectern to center of the room in front of Dais. Estimated Cost: \$308
 - c) Relocate the on-duty police officer to adjacent staff desk to facilitate a quicker response to any physical attack or threat upon dais or employees. Estimated Cost: None

This report is confidential; the disclosure of its contents would be contrary to the public interest.

This report is therefore unavailable for public inspection.

- d) Install an ACS card-reader on the council side of the door to the rear of the Dais with programming to insure the door automatically unlocks upon activation of the fire alarm system for egress. Estimated Cost: \$1,832
 - e) Provide card-access to Council members to the saferoom behind the dais. Estimated Cost: None
6. The Dais in the City Council chambers are not protected from a ballistic attack. Install Kevlar behind the dais to provide L3 ballistic protection of Municipal Staff and the City Council Members. Estimated Cost: \$7,080
7. The dais in City Council chambers allow direct access from the sides by visitors. Install half walls and doors on the side of the Dais to prevent public access to Municipal Staff and City Council Members. Estimated Cost: \$8,625
8. Segregate employee and public parking. Install a 6-foot-tall chain link perimeter fence around the current city employee parking area. Install two 12 foot vehicle entry/exit swing gates incorporating into the facility ACS with one-way traffic around the south and east side of the facility. Estimated Cost: \$132,888
9. The south side of the facility has a high-speed avenue of approach and the public entrance is subject to vehicle ramming due to the handicap ramp.
- a) Establish on the south side of the facility an eighty-foot-long, three-foot-tall decorative berm with a flat concrete wall facing the road side to provide adequate protection from vehicle ramming. Estimated Cost: \$36,983
 - b) Install twenty K-8 rated bollards on the north side of the facility to provide adequate protection. Install eight K-4 rated bollards on the west side of the public entrance. Estimated Cost: \$63,123
10. The current CCTV footage retention is 60 days. Reduce the CCTV footage retention to 30-days city-wide (industry standard) to curb liability and increase video storage for future cameras. Estimated Cost: None
11. Most cameras utilized in the facility are Analog based and do not provide an adequate resolution or field of view. Upgrade the 35 analog cameras in the municipal building to IP base high definition cameras to provide maximum better resolution for the video coverage. Estimated Cost: \$64,449
12. There is no visitor management system for the Municipal Building. Activate the visitor management software for the facility security management system, install a workstation at the receptionist desk and issue temporary adhesive credentials for guests. Estimated Cost: \$2,285
13. The intergraded security system is currently at 65% utilization capacity and the recommended security enhancement will exceed its current operational limits. Upgrade the

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

Professional version of the Enterprise version as soon as possible to provide for security system upgrades. Estimated Cost: \$11,600

14. All security system management duties currently reside with the IT director. Once the position of Director of Security is established and filled moved all security system management duties to that position. Estimated Cost: None
15. The facility utilities are not properly secured when unattended and are susceptible to tampering or sabotage.
 - a) Install a biased magnetic switch on the gates to monitor the open or closed position of the fence at the Municipal Building. Ensure the gates are properly secured when not in use with a high security padlock. Estimated Cost: \$2,707
 - b) Fabricate a metal cage enclosure that can be locked to protect the main gas supply from tampering. Estimated Cost: \$1,286
16. The portion of the facility lighting does not meet the Illuminating Engineering Society (IES) industry standards for proper lighting level. Coordinate with building engineering staff to repair or replace the non-operational lights in the employee parking area and replace the lighting on the center lighting fixture adjacent the flag poles to provide adequate illumination for the facility. Estimated Cost: \$9,844
17. The facility has not developed written procedures for the emergency shut-down or exhaust of air handling systems. Establish emergency shut-down of the facility air handling systems. Install emergency shut-off controls at the receptionist workstation and in the mail room. Estimated Cost: \$1,640
18. The current office configuration does not prevent direct access to the admin employee work areas on the first or second floor. Use knee walls and half doors to establish a physical boundary to the admin employee work area. Estimated Cost: \$8,610
19. There is no CCTV surveillance signage posted at the facility. Post twelve "Video Surveillance in Use on These Premises" signs to advising of CCTV surveillance as a crime deterrent. Estimated Cost: \$2,930
20. The facility does not have adequate IDS protection. All rooms on the ground floor with windows are not protected. Install 19 motion sensors to provide adequate intrusion detection for the facility. Estimated Cost: \$25,641
21. The basement perimeter entry door cipher lock is set to the factory default code.
 - a) Immediately change the cipher lock code. Estimated Cost: None
 - b) Install an ACS card-reader on the door with programming to insure the door automatically unlocks upon activation of the fire alarm system for egress. Estimated Cost: \$1,832

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

22. The City IT data center doors are equipped with large glass panels which does not protect City critical assets. Install two solid core doors to provide adequate protection. Estimated Cost: \$9,170

6.3. Recreation Center Recommendations:

1. The facility does not have adequate CCTV coverage for critical areas.
 - a) Install one IP camera in the safe room to view the safe and funds processing, one IP camera in the Facility Supervisors office where patrons' privileges are terminated and one IP camera in the north hallway. Estimated Cost: \$5,524
 - b) Install three IP cameras in the pool and hot tub area, one in the weight room on the second floor, two for the Children's pavilion interior, three exterior of the facility to provide coverage of the west and south sides of the building. Estimated Cost: \$25,439
 - c) Replace the eleven analog cameras with IP cameras to provide adequate and clear views of the facility CCTV images. Estimated Cost: \$20,254
2. The facility is not equipped with a duress system. Install twelve duress buttons in the following locations, 4 water proof in the pool and hot tub areas, one in the Facility Supervisors office, three in the Children's Pavilion, and four at the receptionist front desk. Estimated Cost: \$10,044
3. The public door to the admin offices is not equipped with means of observation to view the public side of the door. Install a wide-angle peephole in the door. Estimated Cost: \$69
4. Ten perimeter and interior doors are not equipped with ACS and require a key for access. Install ACS on the following doors, The Community Room hallway entry, the public entrance to the Children's Pavilion, The Children's Pavilion Gate, the Center community room door, both interior and exterior Pool chemical storage room doors, the two exterior doors to the lap pool, the south patio door to the pool area and the south patio gate. Estimated Cost: \$36,463
5. The south patio gate does not operate properly and can be opened from the exterior allowing unauthorized access to the pool area during operational hours. Reinforce the center mullion; install a latch-protector plate to deny access to the locking hardware, and three feet of wire mesh welded to the fence panel adjacent the gate to prevent reach-over access to the panic hardware. Estimated Cost: \$1,242
6. The Children's Pavilion playground gate panic hardware can be is easily accessed from the outside of the fence line. Install a latch-protector plate to deny access to the locking hardware, and three feet of wire mesh welded to the fence panel adjacent the gate to prevent reach-over access to the panic hardware. Estimated Cost: \$806

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

7. The Children's Pavilion interior half door is equipped with a lever handle on the public side of the door for access. Deactivate the lever handle and install a remote release at the receptionist counter, an electric strike on the door to limit access to the authorized personnel in the main child care area. Estimated Cost: \$1,026
8. The landscaping outside the Children's Pavilion playground does not prevent direct observation by visitors. Install additional tall plants/grass around the exterior of the playground fence to prevent direct observation of children on the playground. Estimated Cost: \$1,354
9. The main conference room interior door is equipped with a large observation window and is used for public events and community study sessions. Replace the interior door with a solid wood core door and a wide angle peephole to provide adequate protection to the admin area. \$4,380
10. The facility IDS is not equipped with alarm sirens. Install six local intrusion alarm sirens both interior and exterior of the facility to annunciate when the IDS is activated. Estimated Cost: \$4,806
11. The status of the perimeter doors is not monitored locally during operational hours. Enable the monitoring/signal station at the front reception supervisors' desk to alert management of hold open door alarms to restricted areas and select perimeter doors during operational hours. Estimated Cost: None
12. The facility electronic security systems do not have at least 4 hours of UPS capability.
 - a) Install a UPS capable of 4 hours backup. Estimated Cost: \$1,233
 - b) Install a small emergency generator to provide sufficient power during power outages. Estimated Cost: \$17,834
13. The pool areas are not equipped with an effective mass notification system. Coordinate with IT to install four loud speakers capable of being integrated with the facility VOIP phone system. Estimated Cost: \$4,077
14. The facility does not have adequate IDS protection. All rooms on the ground floor with windows are not protected. Install 12 motion sensors to provide adequate intrusion detection for the facility. Estimated Cost: \$19,746
15. The reception desk does not prevent unauthorized access to the facility.
 - a) Install two heavy duty swing gates at the end of the front reception desk to prevent unauthorized access. Estimated Cost: \$4,650
 - b) Install two optical turnstiles (with arms) at the end of the front reception desk to prevent unauthorized access and limit agency liability. Estimated Cost: \$34,060

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

16. The portion of the facility lighting does not meet the Illuminating Engineering Society (IES) industry standards for proper lighting level. Coordinate with building engineering staff to repair or replace the non-operational lights in the north parking area and install lighting on the south side of the facility to provide adequate lighting for the facility perimeter.
Estimated Cost: \$12,740

6.4. Active Adult Center Recommendations:

1. The facility has six perimeter doors and visitor frequently exit through them. Restrict public entry and exit to the east and west lobby doors only. Install local door/alarm sounders and signage on the Prospect hall and Aspen Room exits. Estimated Cost: \$636
2. The kitchen and east public entry door are equipped with single key locks and staff frequently utilizes these doors. Install ACS of the two doors to allow staff more entry points. Estimated Cost: \$5,233
3. The kitchen door is not equipped with a method of observation to view the exterior and there are frequent deliveries at this door. Install a wide angle peephole to observe the exterior of the door prior to opening. Estimated Cost: \$69
4. The perimeter of the building has excessive plant/foilage growth which provides for hiding spots. Remove all plant/foilage for at least three feet from the building and trim existing plants to a low height to protect staff and visitors afterhours. Estimated Cost: \$2,500
5. The facility must log on directly to individual camera IP address to view images. Camera logon and passwords are generic. Management cannot view video archives locally. Install a video management system (VMS) in the supervisors' office to monitor existing cameras properly. Establish proper logon and password policy's for accessing the IP addressed cameras. Estimated Cost: \$3,475
6. The in floor safe is not capable of multi-user and audit capability. Replace the existing combination dial with an electronic keypad with multi-user and auditable capability. \$631
7. The office currently leaves the cash drawer in the reception desk after hours. Properly secure the cash drawer in the safe room after hours which is monitored by the facility IDS. Estimated Cost: None
8. The vehicle key control box is located in the Recreation Supervisors office. Relocate the vehicle key cabinet to the inside of the safe closet to provide an additional layer of security. Estimated Cost: \$57
9. The IDS is not equipped with alarm sirens. Install two local alarm sirens both interior and exterior of the facility to annunciate when the IDS is activated. Estimated Cost: \$1,606

This report is confidential; the disclosure of its contents would be contrary to the public interest.

This report is therefore unavailable for public inspection.

10. The CCTV system does not provide adequate coverage of the facility or have 4 hour of backup power.
 - a) Install four additional IP cameras to provide a full view of the north parking area, the east and south entrance and exits and adjust the views of the current cameras to properly cover the remainder of the perimeter doors. Estimated Cost: \$12,231
 - b) Install a UPS capable of 4 hours backup. Estimated Cost: \$1,233

11. The portion of the facility lighting does not meet the Illuminating Engineering Society (IES) industry standards for proper lighting level. Coordinate with building engineering staff to repair or replace the non-operational lights in the parking areas to provide adequate illumination for the facility. Estimated Cost: \$1,804

Appendix E – References and Acknowledgements

1-14-18 Memorandum of understanding (Parks and Recreation)
1-14-18 Recreation Center Code of Conduct (Parks and Recreation)
1-28-18 Rental Guidelines (Parks and Recreation)
Policy 2-15 Disciplinary Issues with Rec Ctr Patrons (Parks and Recreation)
Anti-harassment and workplace violence policy (City)
Background check (City)
Injury Incident Report (City)
Emergency Action and Safety Plan (City)
Communication Plan (City)
Emergency action plan (Park and Recreation)
Emergency Response Poster (Park and Recreation)
General Security Plan (Parks and Recreation)
IT Consolidated Policy Rev 2018 (IT)
Parks Rules and Regs (Park and Recreation)
Risk Management Plan (Park and Recreation)
Risk Management Policy (Park and Recreation)
Aerial images Google Earth
The Lighting Handbook, 10th Edition, Illuminating Engineering Society (IES)

Appendix F – Acronyms

ACS	Access Control System
CCTV	Closed Circuit Television
CBRNE	Chemical, Biological, Radiological, Nuclear and Explosive
CPTED	Crime Prevention through Environmental Design
DBT	Design Basis Threat
DHS	Department of Homeland Security
DUR	Duress Alarm System
EOP	Emergency Operating Procedures
ESS	Electronic Security System(s)
FBI	Federal Bureau of Investigations
FSL	Facility Security Level
FSP	Facility Security Plan
HAZMAT	Hazardous Materials
HVAC	Heating, Ventilation and Air Conditioning
IDS	Intrusion Detection System
IED	Improvised Explosive Device
ISC	Interagency Security Committee
LOP	Level of Protection
MT	Management Team
NVR	Network Video Recorder
SOC	Security Operations Center
SOP	Standard Operating Procedures
SUV	Sport Utility Vehicle
UCR	Uniform Crime Report
USC	United States Code
VBIED	Vehicle-Borne Improvised Explosive Device

Appendix G – Definitions

Assets: People, information, and property for which the public transportation system is responsible as legal owner, employer, or service provider.

Baseline Threat: The estimate of the relative threat posed to a City facility from an Undesirable Event. Baseline threat is categorized as Low, Medium or High.

Consequences: The severity of impact and probability of loss for a given threat scenario. Consequences may be measured in qualitative or quantitative terms.

Countermeasures: Those activities taken to reduce the likelihood that a specific threat will result in harm. Countermeasures typically include the deployment and training of personnel, the implementation of procedures, the design or retrofit of facilities and vehicles; the use of specialized equipment, the installation of alarms/warning devices and supporting monitoring systems; and communications systems and protocols.

Crime Prevention: The systematic study of the interrelationships among those who commit crime, the location where crime occurs, and the victims of crime to identify patterns, and develop operational and design/engineering strategies to reduce the likelihood of crime and public fear.

Design-Basis Threat: A profile of the type, composition, capabilities, methods (tactics, techniques, and procedures), and the goals, intent, and motivation of an adversary upon which the security engineering and operations of a facility area based.

Facilitating Event: An activity or action associated with the pre-planning or preparation for an event, which potentially increases the likelihood of success of an Undesirable Event by making it less difficult to achieve and/or assisting its progress.

Level of Protection: The degree of security provided by a particular countermeasure or set of countermeasures. Levels of Protection used in this Standard are Low, Medium and High.

Level of Risk: The combined measure of the threat, vulnerability, and consequences posed to a facility from a specified Undesirable Event.

Risk: A measure of potential harm from an Undesirable Event that encompasses threat, vulnerability, and consequence.

Security Breach: An unforeseen event or occurrence that endangers life or property and may result in the loss of services or system equipment.

Security Incident: An unforeseen event or occurrence that does not necessarily result in death, injury, or significant property damage but may result in minor loss of revenue.

Scenario analysis: An interpretive methodology that encourages role-playing by transportation personnel, emergency responders, and contractors to brainstorm ways to attack the system. This analysis uses the

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

results of threat analysis, paired with the system's list of critical assets. Transportation personnel use this analysis to identify the capabilities required to support specific types of attacks. This activity promotes awareness and highlights those activities that can be performed to recognize, prevent, and mitigate the consequences of attacks.

System Security: The application of operating, technical, and management techniques and principles to the security aspects of a system throughout its life to reduce threats and vulnerabilities to the most practical level through the most effective use of available resources.

System Security Management: An element of management that defines the system security requirements and ensures the planning, implementation, and accomplishments of system security tasks and activities.

System Security Program: The combined tasks and activities of system security management and system security analysis that enhance operational effectiveness by satisfying the security requirements in a timely and cost-effective manner through all phases of a system life cycle.

Threat: A threat is any action with the potential to cause harm in the form of death, injury, destruction, disclosure, interruption of operations, or denial of service. Threats include a number of hostile actions that can be perpetrated by criminals, disgruntled employees, terrorists, and others.

Threat Resolution: The analysis and subsequent action taken to reduce the risks associated with an identified threat to the lowest practical level.

Undesirable Event: An incident directed towards a City facility that adversely impacts the operation of the facility, the mission of the agency, or personnel.

Vulnerability: A weakness in the design or operation of a facility that can be exploited by an adversary.

Vulnerability Analysis: The systematic identification of physical, operational and structural components within transportation facilities and vehicles that can be taken advantage of to carry out a threat. This includes vulnerabilities in the design and construction of a given transit facility or vehicle, in its technological systems, and in the way it is operated (e.g., security procedures and practices or administrative and management controls). Vulnerability analysis identifies specific weaknesses with respect to how they may invite and permit a threat to be accomplished.

Appendix H - Site Security Plans




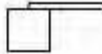



























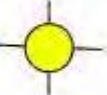

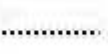

Municipal Building







Annex I – Proposed Location of Sensors and Cameras

Security and Emergency Management Legend

(Icons in RED indicate existing equipment. Icons in BLUE indicate recommended new equipment.)

Video Surveillance	Intrusion Detection	Access Control	Other Security
 Camera-Fixed	 Limit Switch	 Access Keypad	 Drop Arm Barrier
 Camera-PTZ	 Magnetic Switch	 Card Reader	 Automated Gate
 Video Recorder	 Glass Break Sensor	 Card Readerw/keypad	 Magnetic Loop
 CCTV Controller	 Motion Detection Sensor	 Biometric Reader	 Fence/Wall
 CCTV Monitor	 Intrusion Keypad	 Magnetic Lock	 Emergency Exit Device
 Camera w/Keypad	 Siren	 Lock Release Button	 Turnstile
 Camera w/Intercom	 Pressure Mat	 Intercom	 Revolving Door/Mantrap
 Camera w/Card Reader	 Panic Button	 Request To Exit Sensor	 Security Lighting
 Video Multiplexer	 Fence Vibration Sensor	 Security Control Unit	

Life Safety

 Fire Pull Station	 Halon Release	 First Aid
 Fire Extinguisher	 Halon Hold & Release	 Eye Wash
 Fire Hose	 Defibrillator	 Evacuation Chair

Appendix J - Lighting Survey

The results of the Lighting Survey are listed in tabular form below. The lighting locations correspond to marked locations in aerial photographs that follow.

The Municipal Building

	Description of Location	Light Intensity (Lux)
LR1	Sidewalk	H14 V14
LR2	Sidewalk	H14 V15
LR3	Northeast entrance to parking garage	H13 V14
LR4	Sidewalk	H10 V10
LR5	Sidewalk	H13 V14
LR6	East employee entrance	H36 V39
LR7	Alternate employee entrance	H42 V54
LR8	Employee parking circle	H12 V15
LR9	Employee parking circle	H12 V17
LR10	Employee parking circle	H12 V15
LR11	Employee parking circle	H13 V17
LR12	Employee parking circle	H14 V19
LR13	Visitor parking	H15 V22
LR14	Emergency exit	H32 V40
LR15	Visitor entrance	H30 V38
LR16	Employee entrance	H31 V39
LR17	Delivery entrance	H45 V52
LR18	Employee entrance	H32 V40
LR19	Visitor entrance	H40 V52
LR20	Employee entrance	H33 V42
LR21	Plaza park	H12 V15
LR22	Plaza park	H12 V 14
LR23	Southwest entrance to parking garage	H13 V15
LR24	Plaza	H11 V12
LR25	Sidewalk	H12 V14

This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.



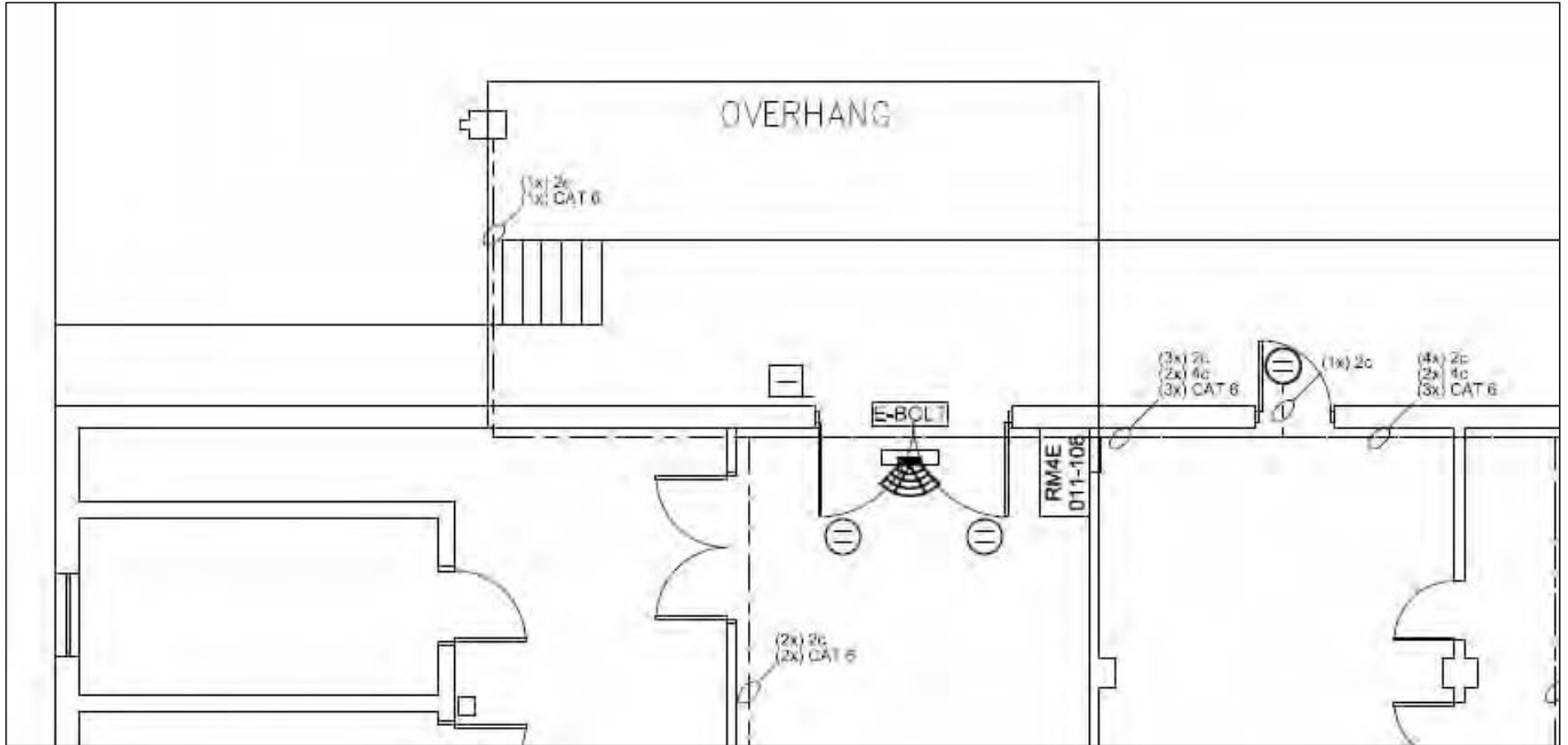
This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.

Appendix K – Site Photos

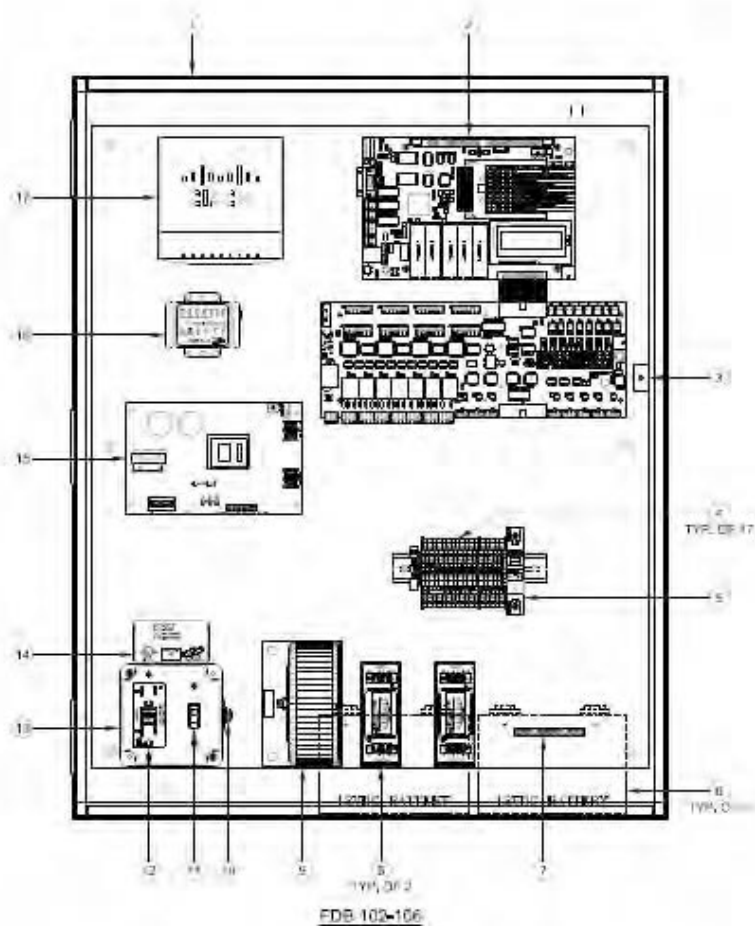
- Photograph 1 – Highspeed avenue of approach looking south.
- Photograph 2 – Highspeed avenue of approach looking north.
- Photograph 3 – Potential vehicle avenue of approach to public entrance doors.
- Photograph 4 – Unprotected site utilities and HVAC.
- Photograph 5 – Employee parking area looking south.
- Photograph 6 – Employee parking parking area looking north.
- Photograph 7 – Public lobby looking north.
- Photograph 8 – Public lobby looking south towards court security screening.
- Photograph 9 – Interior of public entranc door to 1st floor admin area.
- Photograph 10 – Employee work area for 1st floor admin area.
- Photograph 11 – Interior of public entranc door to 2nd floor admin area.
- Photograph 12 – Interior court room.
- Photograph 13 – Interior City Council Chambers.
- Photograph 14 – Waiting are inside court employee work area.
- Photograph 15 – Pool patio area gates that can be opened from the exterior.
- Photograph 16 – Children’s Pavilion playground gate that can be opened from the exterior.
- Photograph 17 – Reception desk with uncontrolled access to the facility.
- Photograph 18 – Children’s Pavilion interior door.
- Photograph 19 – Children’s Pavilion.
- Photograph 20 – Excessive vegetation growth around building.



This report is confidential; the disclosure of its contents would be contrary to the public interest.
This report is therefore unavailable for public inspection.



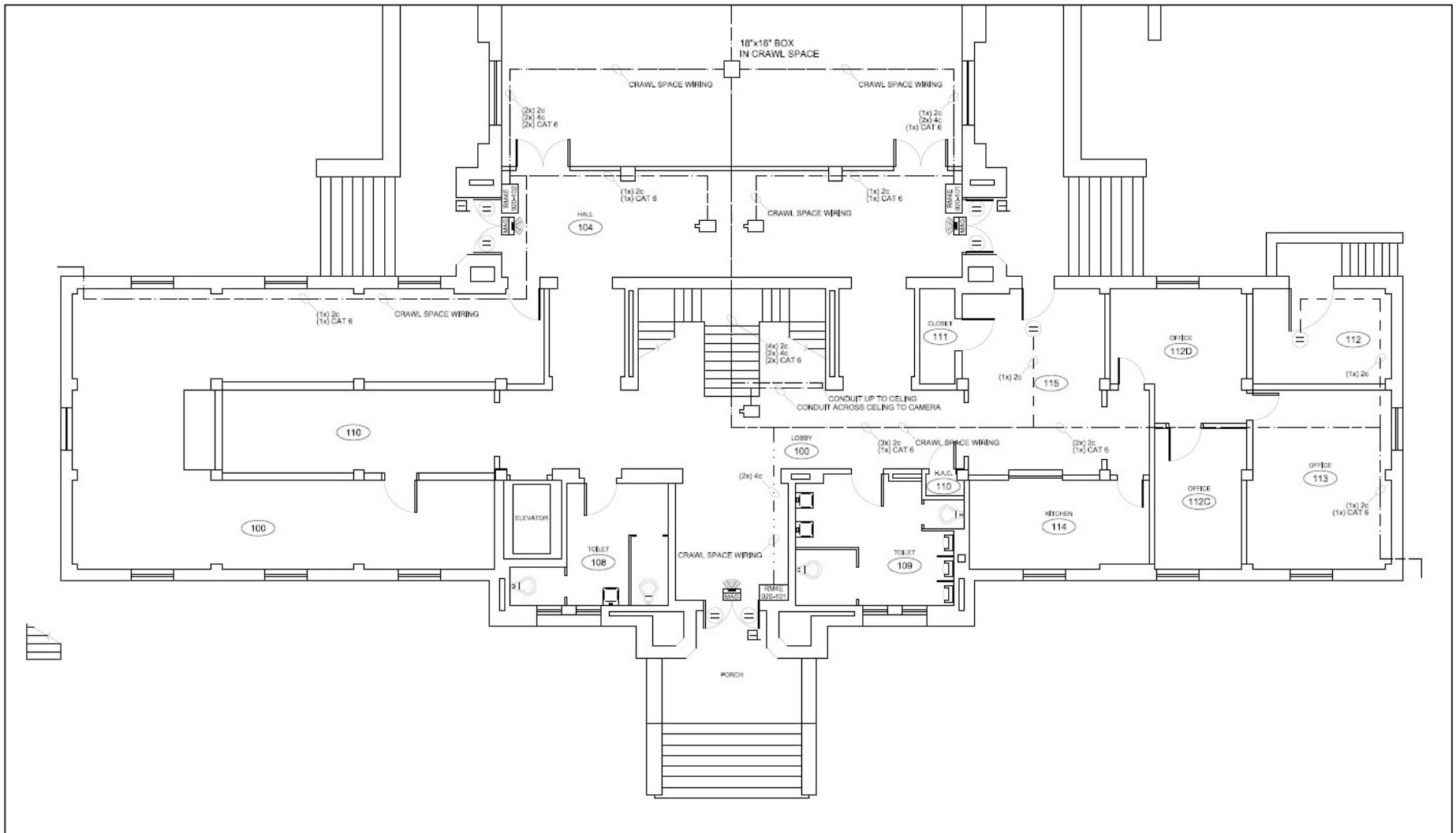
Redacted Example 2 - Example of Floor Plan with Sensor Placement



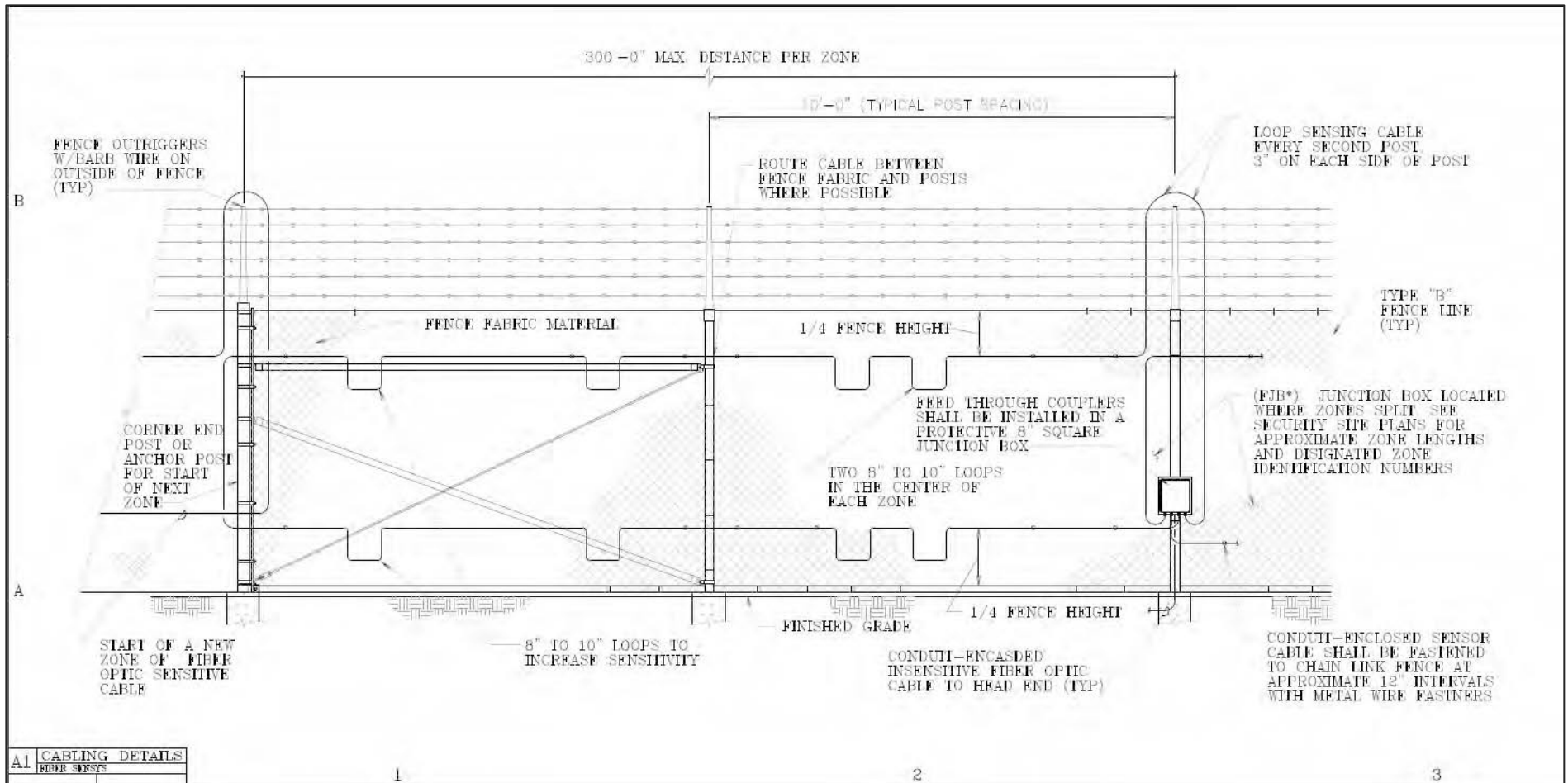
FDB-102-106

FDB 102-106 LOCATED IN SUPPORT FACILITY LIBRARY				
#	MANUFACTURER	COMPONENT	PART/MODEL/STOCK NO.	QTY
1.	HOFFMAN	ENCLOSURE WITH BACKPLANE	A30N24DLP	1
2.	SOFTWARE HOUSE	ISTAR PRO 8 DOOR INTELLIGENT CONTROLLER	STAR006W-84A	1
3.	SENTRON	TAMPER SWITCH	3025T	1
4.	PHOENIX CONTACT	FEED THROUGH MODULAR TERMINAL BLOCK	ATP4JTB 2,54	17
5.	ABL SURSUM	1 AMP CIRCUIT BREAKER	1G1UM	1
6.	INTERSTATE BATTERY	12VDC 12AH BATTERY BACKUP	SLA1105	2
7.	SQUARE D	GROUNDING BUS BAR	PK7GTA	1
8.	DITEK	SURGE PROTECTOR	DTK-3MHC P24-3WB	2
9.	ALTRONIX	24/28 VAC TRANSFORMER - 300 VA	T2428300	1
10.	TYCO ELECTRONICS	5 AMP CIRCUIT BREAKER	W57-KB7MA10-5	1
11.	LEVITON	SWITCH	1451-2W	1
12.	LEVITON	GFCI RECEPTACLE	76367-06	1
13.	CROUSE-HINDS	STEEL OUTLET BOX	TTM03	1
14.	DITEK	SURGE PROTECTOR	DTK-120HW	1
15.	ALTRONIX	12VDC POWER SUPPLY	AL500ULXB	1
16.	DITEK	SURGE PROTECTOR	DTK-MRJ45C5E	1
17.	CISCO	8 PORT ETHERNET SWITCH	SG200-008	1

Redacted Example 3 – Field Distribution Box with Layout and Sensor Component Information



Redacted Example 4 – Example of Floor Plan with Sensor and Wiring Locations



Redacted Example 5 – Example of Fencing with Fiber Optic Sensors



EXHIBIT 15- OPTIONS





EXHIBIT 15 OPTIONS

PROVIDE DETAILED INFORMATION FOR ANY OPTIONAL ITEMS OR SERVICES THAT MAY BE AVAILABLE.

iParametrics has long provided risk and resiliency reports to the utility industry. For those local government organizations responsible for the operation of power generation and transmission facilities connected to the Bulk Electrical System, we can provide NERC-CIP compliant assessments. For Community Water System operators, we have a cadre of security and engineers specialists with the skills and experience of completing the Risk and Resilience Assessment requirements of America's Water Infrastructure Act of 2018.





EXHIBIT 16 - PERFORMANCE MEASURES





EXHIBIT 16

PERFORMANCE MEASURES

For most programs, iParametrics puts in place a customized and formal Quality Assurance Plan which is designed and developed to identify and prevent deficiencies, to document quality activities conducted and corrective actions taken, and to maximize contract productivity and worker performance. This plan includes Key Performance Indicators (KPIs) that help us measure performance.

The plan is based on the principles of ISO 9001-2008 and on the tenet that we are assigned responsibility for quality control and conformance to the criteria of the quality performance requirements through objective evidence. The plan incorporates documented QC activities, verification of quality standards, identification of substandard performance, and resulting management and staff corrective actions sufficient to meet or exceed all requirements of the contract.

For smaller engagements, all employees are held to an internal plan of quality management which follow the same prescribed standards of quality and safety.

An example of this process in action can be illustrated through our Western Area Power Administration PSRA Contract in which we performed random Quality Performance Audits of our field teams assigned within the Sierra Nevada and Mountain Regions. The purpose of these annual exercises was to measure how well our field teams were performing relative to the contract requirements outlined in the SOW for the PSRA contract, the Quality Performance Requirements, and to ensure the services provided were in compliance with those quality performance requirements and met our team's internal standards of quality and safety.

The Quality Audits was performed by a Principal of iParametrics and covered field staff and client interviews and a visual and technical audit of all service elements in accordance with the surveillance criteria contained in the Performance Requirements Objectives for this contract. The field audit was followed by a written report delivered to the client, outlining audit methodology, findings, recommendations, and a status of the program.

PAST PERFORMANCE PROJECT OUTCOMES

WESTERN AREA POWER ADMINISTRATION. In the performance of our WAPA Physical Security Risk Assessment (PSRA) contract, we performed monthly quality meeting with the client and documented timeliness, budget, quality, and effectiveness of the program and its annual PSRAs throughout the year, including:

- Project schedule and project schedule variance



- Budget and budget variance
- On-time completion percentage
- Project cycle time and backlog
- Customer satisfaction (field, regional and HQ, project milestones completed on time with sign off)

We use this data to drive performance improvements through the program. As an example, under the WAPA program, we covered a 15-state region which can be highly impacted by weather events. We created a phased schedule of site assessments based on the historical weather patterns within the region which significantly reduced the amount of “lost-time” assessments due to inclement weather.

Under this program, we completed all annual assessments and reporting cycles ahead of schedule and under budget, while still improving the quality of the product and reacting to continuous changes in scope, regulatory requirements (CIP standards), and threat scenarios.

CITY OF AUSTIN, TX. We use a similar process of collaborative feedback for projects which shorter cycles. Shortly after award of the Austin program, the City Project Manager was diagnosed with an extended illness, and we worked extensively with the City to fill the knowledge gap that her absence left the program.

Through this effort and the efforts of the assessment team, we were able to complete the project nearly 60 days ahead of schedule, while working around all of the end-of-year holidays and the unplanned absence of the customer’s central manager. The work performed under this program developed a threat and risk assessment methodology for Austin that will be used to meet regulatory requirements, while providing the means to identify and mitigate risks to infrastructure.

As evidenced through these examples, iParametrics fosters a culture of continuous improvement through our client and internal quality programs and the regular analysis and reporting of performance measurement data to improve processes, procedures, and client services. These programs have allowed us to maintain a **D&B OPEN RATINGS SCORE** of 94, which places our company in the top 10th percentile of firms in the United States.





EXHIBIT 17 - ADDENDUMS





March 19, 2020

To: All Potential Respondents
From: Randy Worstell, Purchasing Agent
Subject: RFP0920005016 Security Assessment & Design Services

Addendum One

Because the current national crisis and travel restrictions, we having made the following changes to the subject RFB is amended as follows:

1. The final due date and time for "Bid Due" as stated on the RFB cover page is amended to be **April 30, 2020, 1:00 P.M.**

Please acknowledge receipt of this addendum by signing in the space provided below, and return this letter with your bid (do not send back separately).

I hereby acknowledge receipt of this addendum.



Signature

4/29/2020

Date

Paul S. Pelletier

Typed or Printed Name

- A32 The statement in the RFP is correct, we are looking for the estimate time required by State of Iowa staff will be needed to assist the Respondent to complete the Assessment or Design project.
- Q33. On page 15, paragraph 3.3 of the RFP, the State asks for costing information broken down by hourly rate by position. The RFP states this work can be a 6-year contract. Does the State want the hourly rates extended each year showing the cost escalation for inflation per year, per position?
- A33 The State would like hold cost flat year over year but understand that there could be economic factor beyond our control. Rate increases can be addressed during the Master Agreement renewal phase each year.
- Q34. As our great Nation learns to cope and deals with the pandemic of COVID-19 outbreak; will the State of Iowa allow for possible delays respondents may encounter in being able to submit proposal by the March 25, 2020, 1 PM deadline?
- A34. Similar to Q2. See A2.

Please acknowledge receipt of this addendum by signing in the space provided below, and return this letter with your offer (do not send back separately).

I hereby acknowledge receipt of this addendum.



Signature

04/29/2020

Date

Paul S. Pelletier

Typed or Printed Name



April 27, 2020

To: All Potential Respondents
From: Randy Worstell, Purchasing Agent
Subject: RFP0920005016 Security Assessment & Design Services

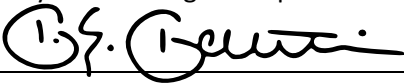
Addendum Three

Because the current national crisis and travel restrictions, we having made the following changes to the subject RFB is amended as follows:

1. Change to Section 2.8 Submission of Proposals process. Please submit the Technical proposal and Cost proposal in separate attachments via email to the Issuing Officer's email: randy.worstell@iowa.gov
 - Because of attachment size limitation within our email systems please eliminate any unnecessary graphics.
 - The cost proposals should be sent as a password protected ".zip" file
 - Do NOT send the password for the ".zip" until after the Technical proposal are scored and you are contacted for the password.
 - The final due date and time for "Bid Due" remain to be **April 30, 2020 @ 1:00 P.M.** as stated in Addendum One.

Please acknowledge receipt of this addendum by signing in the space provided below, and return this letter with your bid (do not send back separately).

I hereby acknowledge receipt of this addendum.



Signature

4/29/2020

Date

Paul S. Pelletier

Typed or Printed Name



EXHIBIT 18- REQUEST FOR CONFIDENTIALITY



Attachment #3
Form 22 – Request for Confidentiality
SUBMISSION OF THIS FORM 22 IS REQUIRED

THIS FORM 22 (FORM) MUST BE COMPLETED AND INCLUDED WITH YOUR PROPOSAL. THIS FORM 22 IS REQUIRED WHETHER THE PROPOSAL DOES OR DOES NOT CONTAIN INFORMATION FOR WHICH CONFIDENTIAL TREATMENT WILL BE REQUESTED. FAILURE TO SUBMIT A COMPLETED FORM 22 WILL RESULT IN THE PROPOSAL TO BE CONSIDERED NON-RESPONSIVE AND ELIMINATED FROM EVALUATION. COMPLETE PART 1 OF THIS FORM IF NO INFORMATION PROPOSAL DOES NOT CONTAIN CONFIDENTIAL INFORMATION. COMPLETE PART 2 OF THIS FORM IF THE PROPOSAL DOES CONTAIN CONFIDENTIAL INFORMATION.

1. Confidential Treatment Is Not Requested

A Respondent not requesting confidential treatment of information contained in its Proposal shall complete Part 1 of Form 22 and submit a signed Form 22 Part 1 with the Proposal.

2. Confidential Treatment of Information is Requested

A Respondent requesting confidential treatment of specific information shall: (1) fully complete and sign Part 2 of Form 22, (2) conspicuously mark the outside of its Proposal as containing confidential information, (3) mark each page upon which the Respondent believes confidential information appears **and CLEARLY IDENTIFY EACH ITEM for which confidential treatment is requested; MARKING A PAGE IN THE PAGE MARGIN IS NOT SUFFICIENT IDENTIFICATION**, and (4) submit a “Public Copy” from which the confidential information has been excised.

Form 22 will not be considered fully complete unless, for each confidentiality request, the Respondent: (1) enumerates the specific grounds in Iowa Code Chapter 22 or other applicable law that supports treatment of the information as confidential, (2) justifies why the information should be maintained in confidence, (3) explains why disclosure of the information would not be in the best interest of the public, and (4) sets forth the name, address, telephone, and e-mail for the person authorized by Respondent to respond to inquiries by the Agency concerning the confidential status of such information.

The Public Copy from which confidential information has been excised is in addition to the number of copies requested in Section 3 of this RFP. The confidential information must be excised in such a way as to allow the public to determine the general nature of the information removed and to retain as much of the Proposal as possible.

Failure to request information be treated as confidential as specified herein shall relieve Agency and State personnel from any responsibility for maintaining the information in confidence. Respondents may not request confidential treatment with respect to pricing information and transmittal letters. A Respondent’s request for confidentiality that does not comply with this form or a Respondent’s request for confidentiality on information or material that cannot be held in confidence as set forth herein are grounds for rejecting Respondent’s Proposal as non-responsive. Requests to maintain an entire Proposal as confidential will be rejected as non-responsive.

If Agency receives a request for information that Respondent has marked as confidential and if a judicial or administrative proceeding is initiated to compel the release of such information, Respondent shall, at its sole expense, appear in such action and defend its request for confidentiality. If Respondent fails to do so, Agency may release the information or material with or without providing advance notice to Respondent and with or without affording Respondent the opportunity to obtain an order restraining its release from a court possessing competent jurisdiction. Additionally, if Respondent fails to comply with the request process set forth herein, if Respondent’s request for confidentiality is unreasonable, or if Respondent rescinds its request for confidential treatment, Agency may release such information or material with or without providing advance notice to Respondent and with or without affording Respondent the opportunity to obtain an order restraining its release from a court possessing competent jurisdiction.


Part 1 – No Confidential Information Provided

Confidential Treatment Is Not Requested

Respondent acknowledges that proposal response contains no confidential, secret, privileged, or proprietary information. There is no request for confidential treatment of information contained in this proposal response.

This Form must be signed by the individual who signed the Respondent’s Proposal. The Respondent shall place this Form completed and signed in its Proposal.

- **Fill in and sign the following if you have provided no confidential information. If signing this Part 1, do not complete Part 2.**

<u>iParametrics, LLC</u> Company	<u>RFB0920005016</u> RFP Number	<u>Security Assessment & Design Services</u> RFP Title
<u></u> Signature (required)	<u>Principal</u> Title	<u>4/27/2020</u> Date

(Proceed to the next page only if Confidential Treatment is requested.)



**178 South Main Street
Suite 100
Alpharetta, GA 30009
Phone: (770) 664-6636
Fax: (770) 664-6696
www.iParameters.com**