Proposal for Consulting Services

for

Security Assessment & Design Services

(RFB0920005016)

Technical Proposal

April 29, 2020

Prepared for:
Iowa Department of Administrative Services (DAS)

Prepared by:
Ron Bundy

trueNORTH consulting group

TABLE OF CONTENTS

Page

EXHIBIT 1 – TRANSMITTAL LETTER 3

EXHIBIT 2 – EXECUTIVE SUMMARY 4

UNDERSTANDING OF THE PROJECT 4
SCOPE OF WORK 4
MANAGEMENT APPROACH – SECURITY ASSESSMENTS 7
MANAGEMENT APPROACH - DESIGN SERVICES 9

EXHIBIT 3 – FIRM PROPOSAL TERMS 11

EXHIBIT 4 – BACKGROUND INFORMATION 12

EXHIBIT 5 – EXPERIENCE 15

EXHIBIT 6 – TERMINATION, LITIGATION, AND DEBARMENT 29

EXHIBIT 7 – CRIMINAL HISTORY AND BACKGROUND INVESTIGATION 30

EXHIBIT 8 – ACCEPTANCE OF TERMS AND CONDITIONS 31

EXHIBIT 9 – CERTIFICATION LETTER 32

EXHIBIT 10 – AUTHORIZATION TO RELEASE INFORMATION 34

EXHIBIT 11 – MANDATORY SPECIFICATIONS 35

EXHIBIT 12– SECURITY ASSESSMENT SERVICES 39

EXHIBIT 13 – SECURITY DESIGN SERVICES 50

EXHIBIT 14 – SAMPLE REPORTS 53

EXHIBIT 15 – OPTIONS 54

SERVICES OVERVIEW 54
SECURITY AWARENESS TRAINING 55

EXHIBIT 16 – PERFORMANCE MEASURES 58

EXHIBIT 17 – ADDENDUMS 59

EXHIBIT 18 – REQUEST FOR CONFIDENTIALITY 67

trueNORTH
consulting group

Exhibit 1 – Transmittal Letter

140 Third Street South, Stillwater, Minnesota 55082
888.650.4580 • 651.430.2772 • www.tncg.com

April 29, 2020

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

Dear Mr. Worstell:

True North Consulting Group, LLC (TNCG) is pleased to provide this proposal to the Iowa Department of Administrative Services for Security Assessment & Design Services (RFB0920005016). TNCG acknowledges receipt of Addendum 1 - 3.

True North Consulting Group services include security assessments, programming, security and technology master planning, emergency management planning and training, detailed design, bidding and negotiations, and contract administration. As a vendor neutral, ASIS credentialed security consultant, we focus on the best fit and best practices for our clients.

Not only do our services fit the process, but our expertise is more diverse than any other consulting firm – security assessments and planning, emergency management planning and response training, suspicious indicators and other security staff training, evaluation of security departments, training, and SOPs, structured cabling for indoor and outside plant; audio/visual systems; multimedia; safety surveillance, access control, and intrusion; wired and wireless networking technologies; network security; server and desktop virtualization; disaster recovery technology; and data center design.

TNCG's representative:

Authorized Representative and Point of Contact:
Ron Bundy, Sr. Strategy Consultant
140 Third Street South
Stillwater, MN 55082
(651) 705-1241
ron.bundy@tncg.com

We have submitted one original and one flash drive in PDF of our technical and cost proposals in separately sealed envelopes, as requested. We look forward to the opportunity to work with you. If you have any questions or if we can be of assistance in any way, please feel free to give me a call at (651) 705-1241 or ron.bundy@tncg.com.

Sincerely,

Ron Bundy, Director | Sr. Strategy Consultant
True North Consulting Group, LLC

Exhibit 2 – Executive Summary

Understanding of the Project

True North Consulting Group, LLC understands the Iowa Department of Administrative Services (DAS) seeks to engage with an independent, qualified security consulting firm to perform Optimization Security Assessments & Plans and/or possible Facility Security System Design Services on facilities to be determined at a later date.

Objectives include:

- Identify security-related threats from internal and external sources (e.g., access control, intrusion detection, video surveillance and monitoring, lock and key control).
- Identify and recommend actions to repair, upgrade, or expand existing systems/solutions to mitigate risk.
- Provide design services for facilities and/or parking lots as needed.

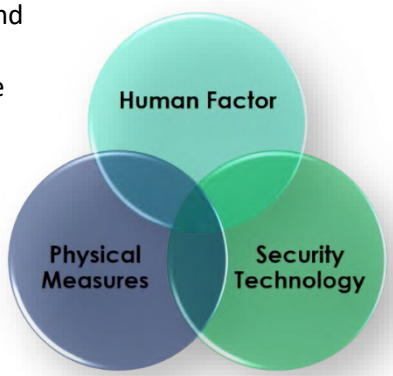
Scope of Work

The scope of work may include, but may not be limited to:

- Conduct security assessments to identify and assess threats from both internal and external sources
- Assess existing physical security systems
    - Access control
    - Intrusion detection
    - Video surveillance, monitoring, storage
    - Lock and key control
- Develop prioritized recommendation actions to repair, upgrade, or expand existing systems/solutions to mitigate risk or eliminate threats
- Provide design(s) for recommended physical security improvements as needed

TNCG Threat, Vulnerability, and Risk Assessment Methodology and Process

TNCG believes we have created a unique, holistic approach to security and risk mitigation professional services. We believe three key areas have a direct impact on the quality and success of a security program. The three areas are Technology, Human Factor, and Physical Security. Each of these areas is interrelated, and addressing only one of these areas does not create a complete solution.



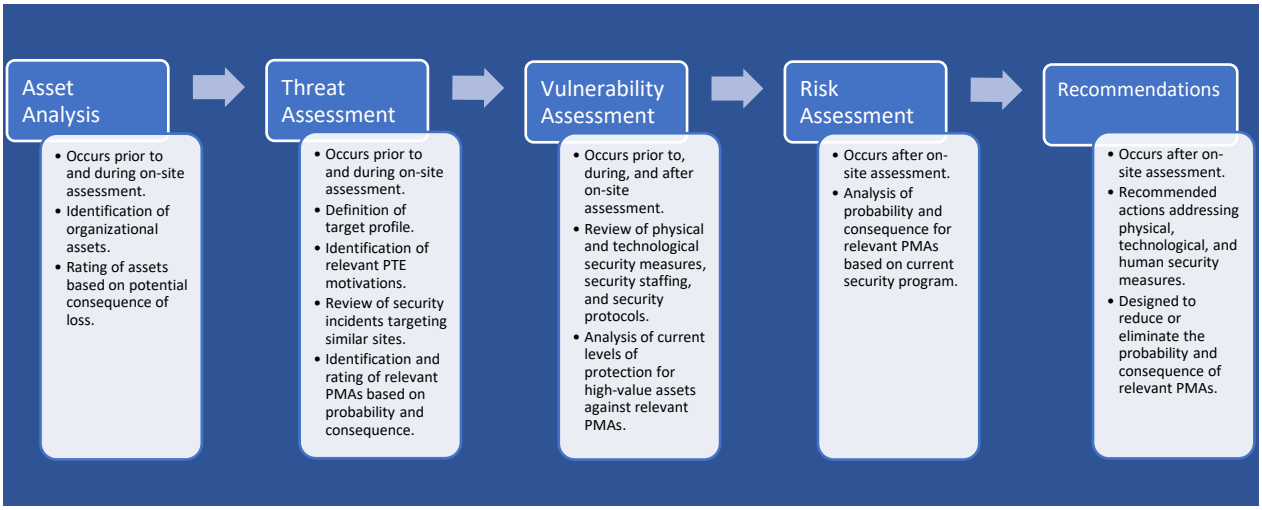
Security Technology has improved dramatically to help security professionals observe and secure more areas and spaces efficiently and effectively. The ability to leverage existing technology infrastructure has been a dramatic improvement as well, improving security at more effective costs.

Physical Measures is most commonly referred to as a means to accomplish security goals. We believe this is a very important part of the security process. Using a layered approach to security and accomplishing the goals of the client through this approach is very important. Access control, gates, fencing, landscaping, and cameras are many different physical items that we see used to help accomplish these goals.

The final and most often overlooked layer of security is the ***Human Factor***. We believe that the best asset is people. They are not only the most valuable asset to protect but also a key in recognizing or understanding potential problem areas and behavioral threats.

We assess security risk based on **threat, consequences of loss/negative impact to most critical assets, and identified vulnerability** in all three domains of security (technology, physical measures/design/layout, and human factor/operations/protocol/training and procedures).

To provide clients with the best possible end-product, we have developed our proprietary, multi-phased methodology for information gathering, risk analysis, and reporting.



Our recommendations are prioritized by their ability to reduce most critical risk across the entire organization.

RISK ASSESSMENT MATRIX				
SEVERITY / PROBABILITY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	High	High	Serious	Medium
Probable (B)	High	High	Serious	Medium
Occasional (C)	High	Serious	Medium	Low
Remote (D)	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Medium	Low
Eliminated (F)	Eliminated			

Risk Assessment Matrix

The Threat and Vulnerability Risk Analysis Matrix allows stakeholders the opportunity to assess consequences in terms of severity of impact and probability of occurrence for a given threat. The matrix is further color coded, indicating and organizing the resulting consequences into categories of High, Serious, Medium, and Low. The matrix will enable the decision-makers to prioritize the most serious threats / vulnerabilities requiring resolution and is serving as the basis for prioritizing our recommended solutions.

This matrix is being used not only to assess the current risk-based on identified deficiencies but also to provide POST implementation risk rate, i.e., after implementing our recommended mitigating measures.

We can also provide a method for tracking the implementation of measures included in the comprehensive safety and security plan and the impact of the implementation on the State's overall level of risk.

Priority	Recommendation	Percent Implementation	Total Percent Risk Reduction	Start Date	Last Update	Date Complete
1	Security Staffing and Deployment: [redacted]	100%	15.5%	5/18/2017		1/22/2018
2	VMF: Security Staffing.	70%	10.2%	4/1/2017	4/1/2017	
3	VMF: Perimeter Access Control	60%	8.7%	4/1/2017	4/1/2017	
4	VMF: Vehicle Access Control	0%	0.0%			
5	VMF: Personnel and Visitor Identification.	80%	11.6%	4/1/2017	4/1/2017	
6	[redacted] Video Surveillance System.	60%	7.3%	4/1/2017	4/1/2017	
7	VMF: Security Awareness.	80%	9.7%	4/1/2017	4/1/2017	
8	VMF: Building Access Control – Access Points.	0%	0.0%			
9	VMF: Video Surveillance System.	100%	11.0%	4/1/2017		12/1/2017
10	VMF: Building Access Control – Visitor Management.	100%	10.8%	6/10/2017		9/12/2017
11	[redacted] Metal Key Management.	100%	9.1%	3/11/2017		4/10/2017

	Total Original Numeric Risk	Total Remaining Numeric Risk	Total % Risk Reduction
Organization Total	24611	10755.543	56.29782%
[redacted]	16145	7761.825	51.92428%
[redacted] Facility	8466	2993.72	64.63835%

Management Approach – Security Assessments

Phase I – Physical Security Assessment - Project Initiation

TASK 1 - Our work would begin with a Project Initiation conference call with the following subtasks:

a. Introduce TNCG team members and reiterate their roles.

b. Review the scope of work with DAS and identify the key contact(s) with whom TNCG would work.

TASK 2- Formulate checklists of needed information and provide those to DAS for completion. Checklists may include requests such as:

a. Listings of key contact personnel

b. Building floor/Open Area Site plans

c. Organizational policies/Written security policies and procedures

d. Description of existing security infrastructure by location/area

TASK 3- Review the data and prepare for on-site assessment.

Phase II – Physical Security Assessment - On-Site Security Assessment

Upon completion of data collection, TNCG will proceed to conduct on-site security assessments for all locations. The assessment will include observation, data collection, and interviews with necessary staff. The information collected as part of the security systems assessment will be incorporated into the final comprehensive assessment report.

TASK 4- Work with key personnel to review current policies, procedures, and processes to identify security objectives for DAS.

a. Assess current readiness/awareness levels and training for staff.

b. Identify and classify risks.

c. Identify strengths and weaknesses.

d. Define triggers.

e. Analyze gaps.

TASK 5- Conduct interviews and/or focus groups with key stakeholders necessary to clarify, identify, and validate issues and challenges.

TASK 6- Discuss the status/development of policies, procedures, and processes effectiveness of implementation.

a. Review existing emergency/crisis management plans.

b. Review and discuss effectiveness and use of Notification and Warning System.

c. Meet with local law enforcement personnel to discuss security.

d. Review response alternatives.

TASK 8- Conduct on-site security assessment for identified areas that will include observation, data collection, and interviews with necessary staff for physical security for:

a. Internal & External

b. Visit sites to examine and document existing conditions, equipment and infrastructure, and determine device locations. Observations are to include:
   i. Description of site
   ii. Description of the physical properties (gates, fencing, etc.)
   iii. Description of the surrounding area (neighborhood, adjacent structures, local businesses)
c. Conduct a review of physical security for facilities and open areas, including supporting infrastructure and equipment, video surveillance, access control, lighting, building entry/exit areas, and other security equipment or systems as applicable.
d. Discuss recent security incidents, and identify threats, risks, and the likelihood of future security incidents based on input from DAS and local law enforcement personnel.

TASK 9 - Present results for staff for comments and feedback on the overall process.

TASK 10 - Conduct assessment of existing network connectivity for security systems.

a. Review communications and security systems and configuration.
b. Assess the capability to handle additional security equipment and integration with the existing network.
c. Provide draft findings and recommendation.

Phase III – Physical Security Assessment - Analysis and Report Development

TASK 11 - Review and discuss:

a. Overall findings from on-site security assessment
b. How existing physical and security technologies and location placement(s) meet DAS requirements
c. Current security systems and/or equipment functionality
d. Video surveillance, video management, access control, lighting systems
e. Content storage and access best practices
f. 'Standards' for future systems expansion and implementation based on locations in building(s), i.e., ingress, egress, halls, stairwells, etc.
g. Building modification needs

TASK 12- Develop prioritized recommendations based on the information collected, stakeholder interviews, and industry-best practices, including:

a. ASIS Protection of Assets Manual
b. FEMA
c. National Crimes Prevention Council
d. National Institute of Justice

TASK 13- As part of the security systems assessment, provide recommendations to replace, re-purpose, or enhance existing systems.

TASK 14- Develop budgetary estimates for recommendations for areas of improvement and implementation strategies.

TASK 15- Develop and deliver a draft Security Assessment Report, including cost estimates for recommendations presented.

TASK 16- Review report with DAS and then make any modification necessary before submitting the final assessment with cost estimates and next recommended steps.

TASK 17- Final comprehensive report will include recommended upgrades, gap analysis, migration strategies, timetables, and cost estimates for security technologies.

TASK 18- (Optional) Present the final comprehensive report to DAS management. (TNCG can provide a closed session of findings and an edited findings open session for the public.)

Management Approach - Design Services

TASK 1- TNCG will discuss and coordinate with DAS the requirements for specification/standard documents. These specifications/standards will be used for future remodeling projects or new construction at facility sites as needed. The specifications/standards will include (but may not be limited to):

a. Security Protocols
b. Entry/Exit Areas
c. Video Surveillance, Monitoring, and Storage
d. Access Control
e. Intrusion Detection
f. Lock and Key Control
g. Alarm Systems
h. Lighting*

**For Lighting, TNCG will provide standards limited to lighting levels and general lighting technology (LED).*

TASK 2- Produce detailed design drawings, including:

a. Device locations
b. Schedules showing individual make, model, mounting conditions, and other notes
c. Installation details and connectivity diagrams.

TASK 3- Develop draft security specifications/standards that include security protocols, entry/exit areas, lighting, video surveillance, video management, access control, and alarm systems. These specifications/standards will be used for future remodeling projects or new construction. The specifications include:

a. "Front-end" document including:
    i. Information for potential proposers/bidders
        1. Important dates/timeline
        2. Scope of the Project
        3. Information about Pre-proposal/Pre-bid meeting and Addenda
        4. Evaluation criteria
    ii. Submission/response requirements
        1. Bonding/security requirements
        2. Required format for responses
        3. Number of copies
        4. Where and when to submit

iii. Discuss and determine vendor qualification requirements
iv. Terms and conditions (including Agreement form)

b. TNCG will create the Technical Specifications portion(s) of the document to include:
   i. General/background information about the project
   ii. Instructions for submittals required at the time of proposal and the format in which those are to be supplied
   iii. Overall/general technical requirements
   iv. Delivery requirements
   v. Description of materials required (with quantities where appropriate), including brand names to establish equivalency requirements (as needed)
   vi. Specific instructions for installation of systems
   vii. Testing and acceptance criteria
   viii. Documentation requirements
   ix. Proposal/bid form with items for respondents to fill in (including qualifications and pricing information)
   x. Proposal bond form to be submitted with the response
   xi. Sample Performance and Payment bond forms
   xii. Sample Application for Payment forms

TASK 4- Review draft security specifications/standards with DAS and incorporate edits.

TASK 5- Deliver final security specifications/standards to DAS.

TASK 6- Conduct Project Meetings and Coordination, including:

a. **Kick-Off Meeting**: TNCG will chair an initial project meeting to review known expectations and design concepts. The purpose of the meeting is to discuss schedules and implementation strategy expectations, agree on the document requirements document, and agree on the level of detail required on all updated documents.

b. **60% Progress Meeting**: A second discussion will be scheduled to review the 60% drafts of all documents and receive feedback from DAS for inclusion in the final deliverables. The primary focus of this meeting is to review the draft documents format, structure, table of contents, and for DAS to provide feedback on key items prior to completion of the documents.

c. **95% Document Review Meeting**: TNCG will coordinate and present the 95% complete specifications/standards document to DAS. All outstanding feedback will be discussed at this meeting for inclusion in the final documents.

d. **Security Specifications**: TNCG will create security guideline specifications in Division 27 CSI MasterFormat. Specifications will include general product and execution requirements. These documents are intended to be incorporated (with project-specific edits) in future project Construction Documents (CDs).

e. **Project Completion**: At the conclusion of the project, TNCG will provide the completed specifications/standards document and diagrams/detail drawings for each system in electronic format and deliver to DAS.

Exhibit 3 – Firm Proposal Terms

True North Consulting Group, LLC. guarantees the goods and/or services offered in this Proposal are currently available and that all Proposal terms, including price, will remain firm for 120 days as indicated on the RFP cover sheet.

Exhibit 4 – Background Information

1. **Does your state have a preference for instate Contractors? Yes or No. If yes, please include the details of the preference.**

   Answer: No

2. **Name, address, telephone number, fax number and e-mail address of the Respondent including all d/b/a's or assumed names or other operating names of the Respondent and any local addresses and phone numbers.**

   Answer: True North Consulting Group, LLC. (formerly Elert & Associates)

   Ron Bundy, (651) 705-1241, ron.bundy@tncg.com, 140 Third St. S., Stillwater, MN 55082

3. **Form of business entity, e.g., corporation, partnership, proprietorship, or LLC.**

   Answer: True North Consulting Group, LLC. is a Limited Liability Company (taxed as an S Corporation).

4. **Copy of W-9.**

   Answer: Please see W-9 on the following page.

Form **W-9**
(Rev. November 2017)
Department of the Treasury
Internal Revenue Service

Request for Taxpayer Identification Number and Certification

▶ Go to *www.irs.gov/FormW9* for instructions and the latest information.

Give Form to the requester. Do not send to the IRS.

Print or type. See Specific Instructions on page 3.

1 Name (as shown on your income tax return). Name is required on this line; do not leave this line blank.
True North Consulting Group, LLC

2 Business name/disregarded entity name, if different from above

3 Check appropriate box for federal tax classification of the person whose name is entered on line 1. Check only **one** of the following seven boxes.

☐ Individual/sole proprietor or single-member LLC ☐ C Corporation ☐ S Corporation ☐ Partnership ☐ Trust/estate

☑ Limited liability company. Enter the tax classification (C=C corporation, S=S corporation, P=Partnership) ▶ S

Note: Check the appropriate box in the line above for the tax classification of the single-member owner. Do not check LLC if the LLC is classified as a single-member LLC that is disregarded from the owner unless the owner of the LLC is another LLC that is **not** disregarded from the owner for U.S. federal tax purposes. Otherwise, a single-member LLC that is disregarded from the owner should check the appropriate box for the tax classification of its owner.

☐ Other (see instructions) ▶

4 Exemptions (codes apply only to certain entities, not individuals; see instructions on page 3):

Exempt payee code (if any)

Exemption from FATCA reporting code (if any)

5 Address (number, street, and apt. or suite no.) See instructions.
3408 Hillcrest Drive

Requester's name and address (optional)

6 City, state, and ZIP code
Waco, TX 76708

7 List account number(s) here (optional)

Part I Taxpayer Identification Number (TIN)

Enter your TIN in the appropriate box. The TIN provided must match the name given on line 1 to avoid backup withholding. For individuals, this is generally your social security number (SSN). However, for a resident alien, sole proprietor, or disregarded entity, see the instructions for Part I, later. For other entities, it is your employer identification number (EIN). If you do not have a number, see *How to get a TIN*, later.

Note: If the account is in more than one name, see the instructions for line 1. Also see *What Name and Number To Give the Requester* for guidelines on whose number to enter.

Social security number
☐☐☐ – ☐☐ – ☐☐☐☐

or

Employer identification number
4 0 – 5 6 5 1 5 9 2

Part II Certification

Under penalties of perjury, I certify that:

1. The number shown on this form is my correct taxpayer identification number (or I am waiting for a number to be issued to me); and
2. I am not subject to backup withholding because: (a) I am exempt from backup withholding, or (b) I have not been notified by the Internal Revenue Service (IRS) that I am subject to backup withholding as a result of a failure to report all interest or dividends, or (c) the IRS has notified me that I am no longer subject to backup withholding; and
3. I am a U.S. citizen or other U.S. person (defined below); and
4. The FATCA code(s) entered on this form (if any) indicating that I am exempt from FATCA reporting is correct.

Certification instructions. You must cross out item 2 above if you have been notified by the IRS that you are currently subject to backup withholding because you have failed to report all interest and dividends on your tax return. For real estate transactions, item 2 does not apply. For mortgage interest paid, acquisition or abandonment of secured property, cancellation of debt, contributions to an individual retirement arrangement (IRA), and generally, payments other than interest and dividends, you are not required to sign the certification, but you must provide your correct TIN. See the instructions for Part II, later.

Sign Here Signature of U.S. person ▶ Ron Bundy Date ▶ 4-28-2020

General Instructions

Section references are to the Internal Revenue Code unless otherwise noted.

Future developments. For the latest information about developments related to Form W-9 and its instructions, such as legislation enacted after they were published, go to *www.irs.gov/FormW9*.

Purpose of Form

An individual or entity (Form W-9 requester) who is required to file an information return with the IRS must obtain your correct taxpayer identification number (TIN) which may be your social security number (SSN), individual taxpayer identification number (ITIN), adoption taxpayer identification number (ATIN), or employer identification number (EIN), to report on an information return the amount paid to you, or other amount reportable on an information return. Examples of information returns include, but are not limited to, the following:

- Form 1099-INT (interest earned or paid)
- Form 1099-DIV (dividends, including those from stocks or mutual funds)
- Form 1099-MISC (various types of income, prizes, awards, or gross proceeds)
- Form 1099-B (stock or mutual fund sales and certain other transactions by brokers)
- Form 1099-S (proceeds from real estate transactions)
- Form 1099-K (merchant card and third party network transactions)
- Form 1098 (home mortgage interest), 1098-E (student loan interest), 1098-T (tuition)
- Form 1099-C (canceled debt)
- Form 1099-A (acquisition or abandonment of secured property)

Use Form W-9 only if you are a U.S. person (including a resident alien), to provide your correct TIN.

If you do not return Form W-9 to the requester with a TIN, you might be subject to backup withholding. See What is backup withholding, *later.*

5. **State of incorporation, state of formation, or state of organization.**

   Answer: Texas, 3408 Hillcrest Drive, Waco, TX 76708 Federal Tax ID: 46-5651592

6. **The location(s) including address and telephone numbers of the offices and other facilities that relate to the Respondent's performance under the terms of this RFP.**

   Answer: Headquarters Address: 3408 Hillcrest Drive, Waco, TX 76708 Phone #: (512) 451-5445

   Minnesota Address: 140 3rd St. S., Stillwater, MN 55082 Phone #: (651) 430-2772

7. **Number of employees.**

   Answer: 50

8. **Type of business.**

   Answer: Independent Security and Technology Consulting Firm

9. **Name, address and telephone number of the Respondent's representative to contact regarding all contractual and technical matters concerning the Proposal.**

   Answer: Ron Bundy, Sr. Strategy Consultant, (651) 705-1241, ron.bundy@tncg.com

10. **Name, contact information and qualifications of any subcontractors who will be involved with this project the Respondent proposes to use and the nature of the goods and/or services the subcontractor would perform.**

    Answer: N/A

11. **Respondent's accounting firm.**

    Answer: N/A

12. **Awarded Respondent will be required to register to do business in Iowa before payments can be made.**

    Answer: Acknowledged

Exhibit 5 – Experience

1. **Number of years in business.**

   Answer: 36 years

2. **Number of years of experience with providing the types of services sought by the RFP.**

   Answer: 36 years. True North Consulting Group (True North) was founded from the Texas Division of Elert & Associates (E&A), a 36-year-old independent technology consulting firm, headquartered in Waco, TX. In 2018, True North Consulting Group and Elert & Associates merged in 2018 and became one company – True North Consulting Group, LLC.

3. **The level of technical experience in providing the types of services sought by the RFP.**

   Answer: True North Consulting Group, LLC (TNCG) is uniquely qualified to perform all aspects of the services requested from our ASIS-certified and internationally trained security personnel, technology integration specialists, Crime Prevention Through Environmental Design (CPTED) experts, and ASIS certified Professional PSP personnel. Our highly motivated staff of over 50 consultants is dedicated to security and technology consulting. Our consultants hold many certifications and professional affiliations, including:

   - AICP American Institute of Certified Planners
   - APCO Association of Public-Safety Communications Officials
   - ASIS American Society for Industrial Security
   - BICSI Building Industry Construction Services International
   - CBCP Certified Business Continuity Planner
   - CHS-III Certified Homeland Security Professional
   - CISM Certified Information Security Manager
   - CISSP Certified Information System Security Professional
   - CPO Crime Prevention Officer
   - CPP ASIS Certified Protection Professional
   - CPTED Crime Prevention Through Environmental Design Certification
   - CRISC Certification in Risk and Information Systems Controls
   - CSS Certified Security Supervisor
   - Ed.M. Master of Education
   - EE Electrical Engineer
   - ENP-911 Emergency Number Professional
   - FCC General Class Radiotelephone License
   - HSEEP Homeland Security Exercise and Evaluation Program
   - ICIA International Communications Industries Association, Inc.
   - ICT Institute for Counter-Terrorism
   - IEEE Institute of Electrical & Electronic Engineers
   - ISA Israeli Security Academy
   - ITIL V3 Foundations
   - LEED AP Leadership in Energy and Environmental Design, Accredited Professional
   - MEP Master Exercise Practitioner
   - PE Professional Engineer (selected states)

- PMP Project Management Professional
- PSP Physical Security Professional
- RCDD Registered Communications Distribution Designer
- RTBAV Certified Instructor in "Refuse To Be A Victim" Training Program
- USGBC U.S. Green Building Council Membership
- Sandia Labs Vulnerability Assessment Methodology

Safety and Security Division

Key Personnel

- Tony Chojnowski, COO, Project Executive
- Michael Rozin, Principal Project Consultant
- Mindy Sitton, Project Coordinator
- Zvi Kremer, Senior Security Consultant
- Ariel Cohen, Security and Threat Intelligence Analyst
- Ross Greves, Senior Security Consultant
- Brandon Frazier, Senior Security Technology Consultant

Please see individual resumes on the following pages.

Tony Chojnowski, RCDD/OSP, RTPM
Chief Operating Officer

Education
North Central University, Minneapolis, MN

Areas of Expertise
- Technology Systems Project Management
- Premise physical security systems
  - Electronic access control
  - Intrusion detection
  - Video surveillance systems
- Voice, data, and video cabling infrastructure
- Fiber optic systems
- Data center planning and design
- Program management

Training and Certifications
- American Clearinghouse for Educational Facilities – Developed 2-part Webinar for Security on Educational Facilities
- BICSI Registered Communications Distribution Designer (RCDD)
- BICSI Certified Outside Plant (OSP) Designer Certification
- BICSI Registered Telecommunications Project Manager Certification (RTPM)
- Genetec A&E Security Design Summit
- BICSI PM125 Telecommunications Project Management
- BICSI OSP200 Outside Plant Design
- BICSI Grounding & Bonding
- BICSI Outside Plan Design
- ASIS STAM – Video Surveillance Design Certification
- Systimax Design Specialist
- Corning Fiber Optic Design, Installation/Inspection Certification
- Annual ASIS Security Conference Participant
- Annual ISC West Annual Security Participant

Significant Projects
City of Augusta, GA Marshal's Office
Design and manage implementation of new video surveillance and access control security systems and new central command center for city-wide system.

City of Garland
Conducted a city-wide risk and vulnerability assessment for 166 city-owned properties. The assessment was based on the CARVER+S methodology considering three factors of risk: asset value, vulnerability and threat. The risk score for each facility was derived from questions that quantify the CARVER+S categories: Criticality, Accessibility, Recuperability, Vulnerability, Effect, Recognizability + Shock.

Aledo Independent School District
District-wide 10-year technology and security assessment for 2014 bond planning effort. The project included assessing and making recommendations for all facilities and meeting with sub-committees to help determine priorities and estimated system costs across the district.

Aldine ISD, TX
Provide E-rate project management and contract administration services for the 2015 FY. Systems included structured cabling - telecom room build-out, pathway installation, backbone and horizontal installation, and demolition of abandoned system per NEC code; local area network (LAN) - MDF/MC campus network systems, IDF/IC edge network systems, and management systems; and wireless networks – controllers, wireless access points, and coverage and performance.

Manor ISD, TX
Provided a districtwide technology assessment and scope preparation for a 2014 technology bond package. TNCG's design services included districtwide upgrades including structured data cabling, PA/bell/clock, AV multimedia, local sound reinforcement (LSR), and security: intrusion, video surveillance, and access control.

Experience
2014 – Present True North Consulting Group
- Chief Operating Officer

2001 – 2014 Elert & Associates
- 2011 – 2014 Executive Vice President
- 2001 – 2011 Senior Technology Consultant

1993 – 2001 Metro Communication Services, Inc.
- Senior Account Manager

Memberships/Affiliations
- BICSI (Building Industry Consulting Service International)
- ASIS International (American Society for Industrial Security)
- IPVM (IP Video Management & Access Control)

Michael Rozin
Executive Security Consultant

Education
International Institute of Counter-Terrorism
- Counter-Terrorism Studies

Ma'agan Michael
- Hebrew Studies

Israeli Defense Forces
- Combat Sergeants School

Israeli Security Academy
- Specialized Security Agent

Fluent in Russian, Bulgarian, Hebrew, English and basic level in Arabic

Memberships
- American Society for Industrial Security (ASIS)
- Twin Cities Security Partnership (TCSP)
- International Association of Bomb Technicians and Investigators (IABTI)
- Institute for Counter Terrorism (ICT) – Young Professionals

Strategic Skills
- National Improvised Explosives Familiarization, Federal Bureau of Investigation (FBI)
- Understanding Islamist Terrorism, Counter Terrorism Operations Center (CTOC)
- Terrorism Awareness: Protecting Soft Targets, Department of Homeland Security
- Terrorism as it relates to Critical Infrastructure, Joint Analysis Center (MNJAC) with Department of Justice (DOJ)
- Explosives Detection Dog Team- Supervisor and Instructor, Global Training Academy
- Krav Maga (Israeli Defensive Tactics), Law-Enforcement Instructor, Krav Maga Worldwide
- ASP Baton & Handcuffing--Law-Enforcement Instructor, Armament Systems and Procedures

Significant Projects and Achievements
Carrollton-Farmers Branch ISD
Serving as Principal Security Consultant for district-wide Safety and Security Assessment Project, assessing 50 facilities.

Washington Metro Area Transit Authority
Serving as Principal Consultant for System-wide Security Assessment Project, assessing 96 facilities.

Connecticut State Colleges and Universities
Senior Security Consultant and Team Lead for system-wide security assessment project, including security staffing review.

West Linn Wilsonville School District, Oregon
Principal Consultant for district-wide security assessment.

Pinellas Suncoast Transit Authority
Security training. Principal Consultant for system-wide security assessment.

Chicago Office of Emergency Management and Communications
Security Assessment.

City of Garland, Texas
Principal Consultant for city-wide security assessment.

Developed Behavior Recognition Training (Suspicious Indicators Recognition and Assessment (SIRA™).

Developed Counter-Terrorism program for Mall of America, along with additional procedural and technological solutions.

Presented program to the US Congress, House of Representatives – Committee on Homeland Security (8/2008) as a security model for private sector.

Granted "Award for Creative Excellence" (highest employee recognition across all departments), Mall of America (2008).

Experience
2009 – Present True North Consulting Group
- Security Consultant

2009 – Present Rozin Security Consulting
- Security Consultant

2004 – 2005 Ben Gurion International Airport
- Specialized Security Agent / Field Supervisor
  Israeli Airport Authority

2003 – 2004 Tel Aviv
- Security Officer, Ministry of Finance/Modiyin Ezrahi LTD

2001 – 2003 Israeli Defense Forces (IDF)
- Sergeant

Mindy Sitton
Security Consultant

Education
Harvard University Cambridge
- Master of Education

University of Texas
- Bachelor of Science, Elementary Education

Areas of Expertise
Training and professional development for clients on the effective integration of technology into the learning environment
- Program evaluation
- Strategic planning
- Policy evaluation and development
- Personnel appraisal systems
- Grant management and coordination

Training and Certifications
- Harvard Project on Negotiation
- Texas Educator Certificates: Elementary Self-Contained (Grades 1-8); Elementary History (Grades 1-8); Generic Special Education (Grades PK-12)

Presentations
- State-level Presentations on topics such as:
  - State Board of Education Task Force Report on Students with Disabilities
  - Qualitative Research on High-Performing Schools
- Educator Appraisal Process (PDAS)
- Administrator Development and Training (ILD) District and campus-level Presentations on topics such as:
  - SHARS (Medicaid) Billing Policies and Procedures
  - Implementing and Evaluating Behavior Improvement Plans

Significant Projects
City Colleges of Chicago, IL
Reviewed existing security systems and developed a security plan and risk assessment for the City Colleges system-wide, along with individual security plans for all seven colleges. Site-specific plans were developed addressing the unique characteristics and physical parameters of each of the seven campuses, as well as training plans enabling the system as a whole and each campus to provide the highest level of security. In addition, we designed system-wide all hazards safety and security plans and conducted training for public safety personnel.

Connecticut Community Colleges, CT
Reviewed and assessed the technology infrastructure and AV systems throughout its 12 campuses. These assessments also included network electronics, network performance, staffing, and network management. We also developed system-wide technology infrastructure and AV multimedia standards for all CCC facilities. Scope from 2006- 2014 has included numerous campus upgrades, a new science building at the Norwalk Community College campus, and the new Gateway campus, located in New Haven, CT.

Denver Public Schools, CO
Conducted a review of building security for Denver Public Schools. After reviewing and establishing district-wide standards, we were retained to assist in the implementation of recommendations including preparing construction documents for recommended security enhancements.

School District Five of Lexington and Richland Counties, SC
Provided a complete technology design, as well as rough and detailed drawings and specifications for all systems, developed bidding packages, developed budgets, and provided system software and hardware recommendations.

Experience
2009 – Present True North Consulting Group
- Education Consultant

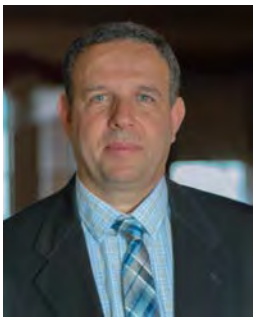
2004 – 2008 Lake Travis Independent School District.
- Special Education Teacher/Project Specialist

1999 – 2002 Region XIII Education Service Center
Division of Statewide Initiative
- Coordinator of Statewide Initiatives

1997 – 1999 Texas Education Agency
Division of Continuing Education and School Improvement Initiatives
- Director of School Improvement Initiatives

Community Involvement
- Austin School for the Performing and Visual Arts
  Member, Advisory Board
- CASA of Travis County
  Court-appointed Special Advocate

Zvi Kremer
Sr. Security Consultant



Education
Loyola University
- Master of Science, Management, International Business, I.S./ Marketing

Tel Aviv University
- Bachelor of Science, Economics and Labor Studies

Areas of Expertise
- Strategic & Operations Planning
- Security Planning & Management
- Multi-site Operations
- Business Development
- Budget Planning, P&L
- Project Management
- Training Development
- Coaching & Training
- Problem Solving
- Presentation, Public-Speaking

Significant Projects
Managed security operations at large scopes, multiple-locations, labor-intensive, regulated, international and high-risk environments including Moscow and O'Hare International Airports.

Developed and implemented security concepts, SOP's, manuals, and training programs for security operations.

Managed multidisciplinary teams (technology, operations, and business) in the process of development and implementation of security technologies and solutions.

Assembled and managed experts' teams for complex airport security consulting projects.

Worked with local and foreign Government agencies to create, coordinate and implement security programs.

Graduate of the "Advanced Security & Anti-Terrorism Management Course", Israeli General Security Agency.

Conducted security assessments and audits for airports, airlines, service providers, and more.

Planned and supported implementation of clients' security programs and services.

Developed and delivered advanced and customized security training programs for employees and clients.

Initiated and executed development and implementation of state-of-the-art Computer-Based-Training programs for security operations and awareness in various industries.

Identified market needs and opportunities for clients' new business development.

Planned and managed the process of responding to solicitations, initiation of unsolicited proposals, pricing, negotiating, and closing of various consulting and operational business opportunities.

Experience
2014 – Present True North Consulting Group
- Contributing Security Consultant

2013 – 2014 Rozin Security Consulting
- Security Consultant

2006 – 2007 Acxiom / Harbinger Airport Technologies Group Inc.
- Director of Strategic Initiatives, Senior Consultant

2001 – 2005 Huntleigh / ICTS USA
- Director of Special Projects, Regional Manager

1995 – 1998 El-Al Israeli Airlines
- Security Manager

Ariel Cohen
Senior Security Consultant

Education
International Institute of Counter-Terrorism
- Master of Science, Counter-Terrorism

Washington University
- Bachelor of Science, Political Science

Areas of Expertise
- Military Leadership and Command
- Translation of Sensitive Documentation
- Logistical Coordination and Support
- Responsible for Fund Allocation and Management
- Squad and Platoon Commander
- On-Going Threat Monitoring
- Terrorist Incident Chronicling
- Terrorism and Violence Trend Analysis
- High-Level Terrorism Threat Assessments

Strategic Skills
- SIRA™ (Suspicious Indicators Recognition and Assessment)
- Intelligence Collection, Analysis & Reporting
- Quantitative Crime and Terrorism Analysis
- Public Speaking
- Military and Security Leadership and Deployment
- Facility Security Benchmarking Analysis
- Security Risk Assessments
- Data Compilation, Manipulation, Analysis, and Presentation
- Threat Intelligence Analysis & Reporting

Significant Projects
Carrollton-Farmers Branch ISD
Description: Ari led a team to provide facility and leadership interviews for twelve CFBISD campuses. Ari's team conducted a comprehensive assessment of campus policies, training, security staffing, emergency preparedness as well as physical measures and security technologies.

Colorado Mountain College
Description: TNCG conducted a security risk/threat and vulnerability assessment including operational and security policy reviews for the College's 12 locations. TNCG reviewed security staffing, operations, and all physical and technological aspects of security. The operations assessment included policy review and identified prioritized alternatives to mitigate identified vulnerabilities.

Chicago Office of Emergency Management & Communications (OEMC)
Description: Threat & Vulnerability Assessment for the 2nd largest Emergency Dispatch Center in the United States.

City Colleges of Chicago
Description: All-Hazards Planning, Security & Risk Assessment

Denver Public Schools
Description: Security Assessment for Denver Public Schools

Rockford Public Schools
Description: Security Threat & Vulnerability Assessment - Gary and several other team members completed a security assessment for all 49 schools. A detailed report, including text and photos of dozens of areas for each school, was provided.

Bureau of Criminal Apprehension (BCA)
Description: RFP for new systems for BCA's move to a new building including data cabling, wireless, security, data center, telephones, audio & video. Guided technology from Schematic Design through Detailed Design, Bidding, Construction Documents, and Contract Administration.

Experience
2014 – Present True North Consulting Group
- Security & Threat Intelligence – Analyst

2013 – 2014 Rozin Security Consulting
- Security Consultant

2007 – 2008 The Institute for Counter-Terrorism
- Open Source Intelligence Monitor

Ross I. Greves, CPP
Public Safety Consultant

Education
Bellevue University, Bellevue, Nebraska
- Bachelor of Science in Security Management

Areas of Expertise
- Public Safety
- 2-Way Radio Systems
- Physical Security Systems;
  - Video Management
  - Electronic Access Control
  - Intrusion Detection
- Emergency Mass Notification
  - Public Marquee Display
  - Workstation, Social Media, Text, Email notification
  - Fire Alarm Integration
- Technology Consulting
- Computer Aided Dispatch (CAD)
- Records Management System (RMS)
- Emergency Management
- Emergency Response
- Business Continuity
- Risk Assessment
- Central Station Design
- Security Control Room Design

Training and Certifications
- ASIS International Certified Protection Professional (CPP)
- Texas DPS Criminal Justice Information Systems
- Salient CompleteView – Enterprise Video Surveillance
- Homeland Security Threat Liaison Officer
- Annual ASIS Security Conference Participant
- FEMA: ICS 100, 200, 700, and 800

Prior to joining True North Consulting Group, Mr. Greves most recently served as the Director of Security for Austin Community College in Austin, Texas. For nearly a decade, he worked to implement a robust and resilient security program to contribute to student safety and overall success in the Central Texas region.

Mr. Greves participated in two Persian Gulf deployments, and one counter-narcotic deployment to Central and South America. His early experience is derived from his installation and maintenance of shipboard RADAR and RF Communications systems. He has served as flight deck fire-fighter/medical corpsman during helicopter evolutions. He gained extensive experience in the design, installation and maintenance of integrated security systems while employed by large security contractors, end-users and independent consulting firms.

Significant Projects
Bates University – Lewiston, Maine
Lead a security assessment effort of Campus Facilities and Off-Campus Housing facilities. Provided technology consulting, design and management to deploy enterprise security systems on and off campus.

Raleigh-Durham International Airport – Cary, North Carolina
Terminal A, Terminal C, General Aviation

Provided consulting services for comprehensive hot-redundant premise access control system upgrade and initial deployment of an enterprise video surveillance system.

Federal Reserve Bank - Districts 11 & 12
System Design and Implementation:

District 11: Provided consulting services to upgrade FRB Dallas cash vault solution. Subsequent projects included an upgrade to District 11's premise access control, video surveillance, and intercom systems.
District 12: Provided security consulting, design and implementation oversight services to expand and enhance a multi-phase security program.

Experience
2018 – Present True North Consulting Group
- Senior Technology Consultant

2009 – 2018 Austin Community College – Austin, Texas
- Director of Security

2001– 2009 Various Consulting
- Senior Security Consultant

1999 – 2001 Security Solutions
- Project Manager

1991-1999 United States Navy
- Electronics Technician, 2nd Class, Surface Warfare

Brandon Frazier CTS, DSCE
Director | Security Technologies

Education
Dunwoody College of Technology, Minneapolis, Minnesota
- Sound, Data and Alarm System Design

Areas of Expertise
- Correctional security systems:
- Jail Programmable Logic Controllers (PLC)
- Human Machine Interface (HMI)
- Intercom
- Advanced System Integration
- Command Center Planning and Design.
- Security Technologies
- Security Master Planning
- Security Migration and Cutover
- Premise physical security systems:
- Enterprise Video Surveillance
- Enterprise Electronic Access Control
- Enterprise Intercom
- Advanced System Integration
- Data and Video Cabling Infrastructure
- Fiber Optic Systems

Training and Certifications
- Avixia CTS certified
- Digital Signage Experts Group DSCE Certified
- Biamp Vocia Certified
- Milestone XProtect Corporate Advanced Certified
- Genetec Security Center Certified
- Exacq Enterprise Certified
- Axis Certified Professional

Significant Projects
Anoka County, Minnesota
Multiple security projects throughout county including video surveillance upgrades at the Government Center Parking Ramp, Human Services Complex, and Homeless Shelter.
Complete fully integrated jail security system upgrade project including PLC, VMS/CCTV, Access Control, intercom, public address and master control remodel. Project include redesigned command center and video wall. Project costs were $1.35m.
Court holding remodel. Expansion of the new jail security systems into the new court holding facility. This included PLC, VMS, Intercom and PA. Project costs were $600k.
Juvenile Detention Facilities security upgrades. Assessment of the existing correctional security system and migration plan for new detention door controls, video surveillance and intercom upgrades. Project costs are estimated at $1m.

Metropolitan Council, Minnesota
Assessment of the existing access control systems for the transit authority and waste management managed under the council which was about to be discontinued and all support halted. Project consisted of approximate 90 buildings and 800 card readers and including the detailed evaluation of the hardware, software, databases, card technologies, power supplies, FTE efficiency and deep integration requirements. The cost of the recommended upgrades exceeded $3M.

US Bank (Vikings) Stadium, Minnesota
Responsible for all security including a fully integrated video surveillance and access control solutions along with multiple command center designs. Performed services from design through contract management including advanced full system commissioning. Project costs were in excess of $5m.

Minneapolis Public Schools, ISD 1, Minnesota
Multiple elementary, middle school and high school projects (35+ buildings) with a unified video surveillance, access control and intercom system. Additional project included writing security standards and standard specifications for district use.

Moraine Park Technical College, Wisconsin
Multi-campus access control upgrade including over 300 intelligent wireless and PoE locksets and over 100 traditional card readers. Threat level integration to enable controlled lock downs for weather (most safe rooms), fire and active shooter threat. Integration to mass notification system for rapid communication of events.

Experience
2018 – Present True North Consulting Group
- Director | Security Technologies

2012 – 2018 Elert & Associates
- Senior Technology Consultant

2006 – 2012 KJWW Engineering
- Technology Designer

2005 – 2006 Uponor Wirsbo
- Residential Fire Protection Designer

2004 – 2005 Master Technology Group
- Project Manager

David Hlusak
Senior Consultant | Security Technologies

Education
Community College of the Air Force
Maxwell AFB, AL
- Electronic Systems Technology

Areas of Expertise
- Enterprise Access Control
- Command Center Planning and Design
- Access Control Migration and Cutover
- Premise physical security systems:
- Enterprise Video Surveillance
- Enterprise Electronic Access Control
- Intrusion Detection
- Parking Management
- Advanced System Integration
- Network Infrastructure
- Special Locking Arrangements
- Secure Card Technologies
- Fiber Optic Planning, Design, Installation

- **Training and Certifications**
- Genetec Security Center Certified
- Lenel Certified Expert – Digital Video
- Prism Video Certified
- Avigilon Control Center Certified
- Milestone Certified Design Engineer
- S2 Security Certified
- Certified Protection Officer
- LEAN Leadership Yellow Belt
- Infection Control Risk Assessment – Healthcare Construction Certified
- Electronic Technicians Association –
- Fiber Optics Installer

Significant Projects
Bay Area Medical Center, Wisconsin
Design services for physical access control and video surveillance systems for greenfield 335K square foot hospital and associated medical office building. Included design of interior spaces, exterior perimeter lot monitoring, door hardware and function coordination, and special locking arrangement requirements.

North Memorial Health, Minnesota
Assessment of the existing access control and video management systems for the safety and security teams. Projects consisted of a broad scope including design and implementation of lockdown controls, parking management access control, ICRA compliant security installation strategies, video surveillance system platform migration plans, and video surveillance system lifecycle replacement.

US Bank (Vikings) Stadium, Minnesota
Responsible for implementation of physical access control and IP video surveillance systems, including planning, programming, configuration, testing, and training. Provided event specific planning and support to maximize system utilization, including provided direct support of Super Bowl LII.

Target Corporation, Minnesota
Manage the Enterprise access control platform strategy, developing best practices, installation standards, and training programs for worldwide user base. Planned implementation and execution strategies for physical access control installations within widely varying environments including retail, distribution, and headquarter locations.

Carlson Companies, Minnesota
Assisted in development of world class security operations center monitoring all corporate headquarter facilities and associated assets. Developed training programs intended to maximize capabilities of the access control platform and video management systems.

Experience
2019 – Present True North Consulting Group
- Senior Consultant | Security Technologies

2015 – 2019 Parsons Technologies
- Senior Security Systems Specialist

2011 – 2015 Target Corporation
- Corporate Security Specialist

2002 – 2010 Carlson Companies [Contract]
- Security Operations Center Manager

4. **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.**

   Answer:

DESCRIPTION OF SECURITY CONSULTING SERVICES PROVIDED BY TRUE NORTH CONSULTING GROUP	
Security Risk Assessments	Comprehensive, risk-based assessments of facilities and security programs utilizing DHS, FBI, and Israeli Shin Bet methodology. Assessments include risk analysis, threat assessment, vulnerability assessments, and mitigation recommendations. The goal of the assessment is to increase our client's ability to prevent, detect, deter, and respond to man-made threats to staff and visitors on facilities.
Threat Assessments	Comprehensive, community-specific threat assessments utilizing DHS and FBI methodology and incorporating up-to-date threat information from local and regional law enforcement, including regional FBI Fusion Center data and information.
Physical Security & Supporting Technology Infrastructure Design and Engineering, Acquisition & Project Management	True North provides these services in the following technologies: o Video Surveillance/CCTV/Lighting o Identity Management o LAN (including Wireless LAN) o Access/Entry Control o Video Management Systems (VMS) o Video Analytics and Biometric Technologies o Alarm Systems/Intrusion Detection/Notification Systems o Communications/Dispatch Systems/Command Center
Security Master Planning	TNCG consultants provide security master planning services, providing our clients with a comprehensive, long-term strategy that covers all aspects of a security operation and provides sequential planning over a period of years to provide a safe, secure environment.
Program Implementation	TNCG consultants will work with our clients on an ongoing basis to assist in the implementation of recommended mitigation strategies and the enhancement of security programs.

5. **Letters of reference from three (3) previous or current customers or clients knowledgeable of the Respondent's performance in providing goods and/or services similar to the goods and/or services described in this RFP and a contact person and telephone number for each reference.**

   Answer: True North Consulting Group (True North) was founded from the Texas Division of Elert & Associates (E&A), a 36-year-old independent technology consulting firm. In 2018, True North Consulting Group and Elert & Associates merged in 2018 and became one company – True North Consulting Group, LLC. Please see the reference letters on the following pages.

Carrollton-Farmers Branch
Independent School District

True North Consulting Group - Reference Letter

September 6, 2018

I am writing this letter to recommend True North Consulting Group (TNCG) for independent consulting services. Carrollton-Farmers Branch ISD has worked with True North Consulting Group on multiple projects in recent years. Chief among these projects is a district-wide comprehensive safety and security vulnerability assessment.

In April 2018, Carrollton-Farmers Branch ISD (CFBisd) issued an RFP for district-wide security assessment of current physical, procedural and behavioral related threats and vulnerabilities by a specialized independent, non-product affiliated security consulting firm. After review of multiple responses and conducting interviews of top 'short-listed' responders, CFBisd's selection team chose to recommend True North as the most qualified k12-focused security consulting firm. To date, the True North team, led by Tony Chojnowski and Michael Rozin, have met and exceeded our expectations.

Specifically, our project included a comprehensive safety & security assessment with an aggressive timeline. The TNCG assessment team included highly trained security professionals conducting comprehensive site assessments and campus leadership interviews for all fifty (50) district facilities.

The feedback from all participants has been overwhelmingly positive. Considering the timing of the facility assessments, interviews and events with local first responders, this type of feedback was surprising and gratifying. It became obvious throughout the process that TNCG will be able to effectively identify and prioritize operational, physical and technology related vulnerabilities in accordance with the aggressive schedule required by our district. We are also confident that their unique approach to assessing the three major elements of a school district security plan; (1) Security Technologies, (2) Physical Measures and (3) the Human Factor, is both relevant and contextualized to our specific needs.

A primary function of any school District is to balance a safe and secure environments with a positive and friendly educational setting. By doing so, a district can safely carry out its charge, and ultimately provide every student with a chance for success. It is my opinion, that True North has the security knowledge, expertise and resources, coupled with the needed K-12 experience, that are required for a comprehensive district-wide security assessment project of this nature.

I would highly encourage you to consider True North for safety & security consulting services for your district and I look forward to a continuing relationship with them on their current and future projects with Carrollton-Farmers Branch ISD.

Respectfully,

David Finley, AIA, ALEP, Chief Operations Officer
Carrollton-Farmer's Branch ISD

CYPRESS FAIRBANKS
INDEPENDENT SCHOOL DISTRICT
LEARN • EMPOWER • ACHIEVE • DREAM

Facilities & Construction Department
11430 Perry Road, Houston, TX 77064

Matt Morgan
Assistant Superintendent, Facilities & Construction

True North Consulting Group - Reference Letter

February 12, 2020

I am writing this letter to recommend True North Consulting Group for independent security consulting services. Cypress-Fairbanks Independent School District hired True North Consulting Group to conduct a district-wide comprehensive safety and security vulnerability assessment.

In August 2018, Cypress-Fairbanks Independent School District (CFISD) issued an RFQ for district-wide security assessment of current physical, organizational, and behavioral related threats and vulnerabilities by a specialized, independent, non-product-affiliated security consulting firm. After review of all responses and conducting interviews of top 'short-listed' responders, CFISD's selection team chose True North as the most qualified k12-focused security consulting firm in November 2018. The True North team, led by Tony Chojnowski and Michael Rozin, met and exceeded our expectations.

Our project included a comprehensive safety & security assessment with an aggressive timeline. To meet the time and budget needs of the district, TNCG worked with the district to conduct comprehensive on-site assessments of prototype schools in the district, as well as schools with unique footprints and district stadiums and administrative facilities. CFISD used the findings of the assessment to develop priorities for the bond funding requests and spending.

The TNCG assessment team included highly trained security professionals conducting comprehensive site assessments and campus leadership interviews for thirty-seven district facilities. Also, TNCG assessed the overall security program for the district as a whole.

Following the facility assessments and interviews with district staff, as well as local responders, the feedback from the process has been overwhelmingly positive. True North helped identify and prioritize operational, physical, and technology-related vulnerabilities. CFISD utilized the findings and recommendations to inform our bond planning. We feel they have the correct approach to assessing the three major, interrelated elements of a school district security plan; (1) Security Technologies, (2) Physical Measures and (3) the Human Factor.

As a school district, it is our job to provide safe learning environments, while maintaining a positive and friendly learning environment where students can succeed. In my opinion, True North has the security knowledge, expertise, and resources, with an understanding of the k12 environment that are required for a comprehensive district-wide security assessment project.

ALEDO INDEPENDENT SCHOOL DISTRICT

June 15, 2017

To Whom It May Concern:

I have worked with Tony Chojnowski and the TrueNorth team while serving two different school districts. In Aledo ISD, True North was an instrumental part of our district-wide comprehensive facility and security assessment in preparation for bond. Once the community passed our bond proposal, True North was very helpful in security and technology design, improvements and owner's representation thru the contract administration phase.

True North worked closely with the architectural firm and provided a district-wide security and technology assessment as a part of a master facilities assessment. They also worked closely with my team to provide a roadmap for the district and presented this plan to the Board of Trustees, paying particular attention to what mattered most – our kids and staff.

While at my previous district (Southlake Carroll), TrueNorth (Previously Elert & Associates-TX) provided design, procurement and owner's representation contract administration services for the deployment of nearly $40M in security and technology projects including district-wide physical measures, security technologies, two data centers, and bell/clock/public address. These projects required many contractors and the True North team successfully worked with our staff to represent our needs and goals across all projects. As they were a part of the project from the beginning assessment efforts, they knew what the district was committed to accomplishing.

As Superintendent, part of my job is to make sure that we are investing in our district and leveraging our investments in technology to maximize the educational experience and increase operational efficiencies.

I strongly encourage you to consider adding them to your team for any assessment, bond planning, training and/or deployment initiatives as they will work with you to understand your current strengths, vulnerabilities and recommended priorities.

Respectfully,

Derek Citty, Superintendent of Schools
Aledo Independent School District
817-271-7839 Direct

1008 Bailey Ranch Road, ALEDO, TEXAS 76008 * 817-441-8327 * 817-441-5144 FAX

Exhibit 6 – Termination, Litigation, and Debarment

1. **Has the Respondent had a contract for goods and/or services terminated for any reason? If so, provide full details regarding the termination.**

   Answer: No

2. **Describe any damages or penalties assessed against or dispute resolution settlements entered into by Respondent under any existing or past contracts for goods and/or services. Provide full details regarding the circumstances, including dollar amount of damages, penalties and settlement payments.**

   Answer: None

3. **Describe any order, judgment or decree of any Federal or State authority barring, suspending or otherwise limiting the right of the Respondent to engage in any business, practice or activity.**

   Answer: None

4. **A list and summary of all litigation or threatened litigation, administrative or regulatory proceedings, or similar matters to which the Respondent or its officers have been a party.**

   Answer: None

5. **Any irregularities discovered in any of the accounts maintained by the Respondent on behalf of others. Describe the circumstances and disposition of the irregularities. Failure to disclose these matters may result in rejection of the Proposal or termination of any subsequent Contract. The above disclosures are a continuing requirement of the Respondent. Respondent shall provide written notification to the Agency of any such matter commencing or occurring after submission of a Proposal, and with respect to the successful Respondent, following execution of the Contract.**

   Answer: None

Exhibit 7 – Criminal History and Background Investigation

The Respondent 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 and consultants who will be involved in the performance of the Contract.

TNCG acknowledges and 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, and consultants who will be involved in the performance of the Contract.

Exhibit 8 – Acceptance of Terms and Conditions

TNCG acknowledges its acceptance of the terms and conditions of the RFP and the General Terms and Conditions without change except as otherwise expressly stated.

Exhibit 9 – Certification Letter

Attachment #1
Certification Letter

April 28, 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 **True North Consulting Group, LLC.** 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 the Agency.

Sincerely,

Ron Bundy

Signature

Ron Bundy, Sr Strategy Consultant
Name and Title of Authorized Representative

04-28-2020
Date

trueNORTH
consulting group

Exhibit 10 – Authorization to Release Information

Attachment #2
Authorization to Release Information Letter

April 28, 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:

True North Consulting Group, 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,

Ron Bundy

Signature

Ron Bundy, Sr. Strategy Consultant
Name and Title of Authorized Representative

04-28-2020
Date

Exhibit 11 – Mandatory Specifications

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

ASIS International
Professional Certification Board

Awards

Ross J. Greves, CPP

the designation of

Certified Protection Professional

in witness thereof this certificate is granted

June 9, 2005

ASIS INTERNATIONAL Advancing Security Worldwide

CPP Certified Protection Professional Board Certified in Security Management

11242 — Certification Number

John W. Schulz, CPP — President

Daphne Philos — Program Director

4.1.2 Respondent must have the ability to perform security assessment of State of Iowa facilities and/or Subs. Yes, TNCG is currently working with the City of Ames performing a similar project and has performed a video surveillance project with the Veterans Home in Marshalltown.

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, True North Consulting Group, LLC. (TNCG) is uniquely qualified to perform all aspects of the services requested from our ASIS-certified and internationally trained security personnel, technology integration specialists, Crime Prevention Through Environmental Design (CPTED) experts, and ASIS certified Professional PSP personnel. Our highly motivated staff of over 50 consultants is dedicated to security and technology consulting.

4.1.4 Respondent must have the ability to Review of 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, True North Consulting Group, LLC. (TNCG) is uniquely qualified to perform all aspects of the services requested from our ASIS-certified and internationally trained security personnel, technology integration specialists, Crime Prevention Through Environmental Design (CPTED) experts, and ASIS certified Professional PSP personnel.

4.1.5 Respondent must have the ability to identify and make recommended actions that mitigate and/or eliminate risk. Yes, True North Consulting Group, LLC (TNCG) is uniquely qualified to perform all aspects of the services requested from our ASIS-certified and internationally trained security personnel, technology integration specialists, Crime Prevention Through Environmental Design (CPTED) experts, and ASIS certified Professional PSP personnel.

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 – see samples.

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

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

4.1.9 Respondent shall respond to assessment request within 48 hours. Yes

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

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

Affidavit of Non-Alliance & Independence

True North Consulting Group, LLC. states:

- We are an independent security and technology-consulting group.
- We sell no hardware or software or any tangible products, including but not limited to locks, alarms, fencing, bollards, doors, window coverings, security systems, networking devices, wireless equipment, telecommunications equipment, or cabling.
- We are not aligned with any manufacturers of the above-listed products or any products.
- We are not aligned with any vendors, or distributors, or representative firms who sell, market, install, program, or subcontract work for the above-listed products, or any products or services.
- We receive no commissions, salaries, or payoffs of any kind from any business entity for services we perform on behalf of our clients, or for products that we may from time to time recommend to our clients on their behalf.

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

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

ASIS International
Professional Certification Board

Awards

Ross J. Greves, CPP

the designation of

Certified Protection Professional

in witness thereof this certificate is granted

June 9, 2005

ASIS INTERNATIONAL Advancing Security Worldwide

CPP Certified Protection Professional Board Certified in Security Management

11242 — Certification Number

John W. Schulz, CPP — President

Daphne Philos — Program Director

4.2.2 Respondent must have the ability to perform facility security system design for the State of Iowa facilities and/or subcontractors. Yes, see 4.1.3.

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, see 4.1.3

.

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, 4.1.3.

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

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

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

4.2.8 Respondent shall not be in the business of selling security systems hardware. Yes, see 4.1.11.

4.2.9 Respondent must adhere to work rules of the applicable facility. Yes

4.3 Post Delivery Documentation

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

Exhibit 12– Security Assessment Services

1. **Describe Respondent's experience in performing security assessments and technical security designs for municipal facilities – reference checks may be used in evaluation of proposals.**

   Answer: TNCG security consultants have been providing governmental agencies security/public safety consulting throughout our 36 years. Our firm employs individuals with Certified Protection Professional (CPP), Physical Security Professional (PSP), Emergency Number Professional (ENP), Certified Business Continuity Professional (CBCP), Project Management Professional (PMP), Certified Technology Systems Designer (CTS-D), Registered Communications Distribution Designer (RCDD), and past law enforcement personnel. We approach our security consulting for our clients from an integrated, holistic approach, addressing physical security measures, security technology measures, and human factor or operational security measures (policies and procedures, human resource utilization, etc.) and the interplay between these three critical areas of security. The goal of our security consulting services is to assist our clients in enhancing the ability to deter, detect, prevent, and respond to all hazards and threats they may face.

2. **Demonstrate experience in conducting security work for government institutions of similar or larger size and scope.**

   Answer: Within the last five years, TNCG consultants have provided system-wide security assessment services to the following:

Name	Location	Size	Scope
Routt County	Steamboat Springs, Colorado	4 Locations	Campus-wide Security Threat, Risk, Vulnerability Assessment including Security Technology Assessment
Nueces County	Corpus Christi, Texas	Courthouse Facility	Security Risk Assessment and Security Master Plan
City of Santa Cruz	Santa Cruz, California	14 Locations	Security Assessment
City of Ceres	Ceres, California	14 Locations	Security Assessment & Design
City of Tamarac	Tamarac, Florida	29 Locations	Security Assessment & Master Plan
Redwood City (currently underway)	Redwood City, California	5 Locations	Security Assessment
City of Englewood/South Platte Water Renewal Partners (currently underway)	Englewood, Colorado	Water Treatment Campus	Campus-wide Security Threat, Risk, Vulnerability Assessment including Security Technology Assessment
Washington Metropolitan Area Transit Authority	Washington, DC	96 Locations	System-wide Security Assessment, including security assessments of facilities in pre-construction phases
New Hanover County School District	Wilmington, North Carolina	47 Schools	District-wide Security Threat, Risk, Vulnerability Assessment

Lake Oswego School District	Lake Oswego, Oregon	10 Schools	District-wide Security Threat, Risk, Vulnerability Assessment
Palm Springs Unified School District	Palm Springs, California	31 Schools	District-wide Security Threat, Risk, Vulnerability Assessment
Carrollton-Farmers Branch ISD	Carrollton, Texas	38 Schools	District-wide Security Assessment
West Linn-Wilsonville School District	West Linn, Oregon	18 Schools	District-wide Security Assessment
Aldine ISD	Houston, Texas	78 Schools	District-wide Security Assessment
Midlothian ISD	Midlothian, Texas	11 Schools	District-wide Safety and Security Assessment
Rockford Public Schools	Rockford, Illinois	49 Schools	District-wide Security Assessment
Kansas City Public Schools	Kansas City, Kansas	40 Schools	District-wide Security Assessment

City of Arvada, Colorado

Project Description: The City of Arvada retained TNCG to assess security and prepare a security master plan including reviewing and establishing one point vs. multiple points of entrance, installation of passive or active screening methods, reviewing and establishing a budget for upgrades of video surveillance, access control, intrusion detection, and all physical security measures (i.e., door locks, bollards, x-ray, magnetometers) along with passive screening and policy & procedures change and review.

Contact: Mr. Kim A. Vagher, Manager of City Facilities, (720) 898-7681, kvaugher@arvada.org

City of Garland, Texas

Project Description: The City of Garland retained True North Consulting Group to assess the security of all City facilities. Specifically, the project included a comprehensive safety & security assessment of selected prototype City facilities, with a CARVER-based methodology for prioritizing security measures for other City facilities aligned with the in-depth threat assessment and analysis conducted by TNCG. Using this methodology, TNCG calculated risk scores for all 165 City facilities. Once risk levels of all City facilities were calculated, TNCG security consultants conducted full SRAs for the high-risk facilities identified by the analysis.

Contact: Ms. Ginny Holliday, Director of Facilities Management, (972) 205-4080, gholliday@garlandtx.gov

Routt County, Colorado

Project Description: True North Consulting Group was retained by Routt County, CO to provide a comprehensive risk assessment. The assessment included an analysis with recommendations regarding the security systems and security operations at the Routt County Campus located in Steamboat Springs, Colorado. The sites included are the Historic Courthouse, the Annex, the Department of Human Services, and the Log Cabin Buildings.

Contact: Mr. Steve Faulkner, Facilities Manager, (970) 870-5218, sfaulkner@co.routt.co.us

City of Tamarac, Florida

Project Description: TNCG developed a security master plan, including a security risk threat and vulnerability assessment for 29 public facilities. Work included a risk-based review of video surveillance, access control, and intrusion detection. In the master plan, TNCG provided risk-based prioritized recommendations, including cost estimates for all City facilities.

Contact: Mr. Levent Sucuoglu, Director of Information Technology, (954) 597-3900, levent.sucuoglu@tamarac.org

City of Santa Cruz, California

Project Description: True North was retained to provide an assessment of city security cameras, video management, and access control systems for City Water Department facilities, oversee implementation at City Water Department facilities, and create a master plan for system implementation across all City facilities.

Contact: Ms. Kimberly Ramirez, IT Project Manager, (831) 420-5030, kramirez@cityofsantacruz.com

Washington Metropolitan Area Transit Authority, DC

Project Description: TNCG was contracted to provide Threat and Vulnerability Assessments (TVA) for all Washington Metropolitan Transit Authority (WMATA) facilities and infrastructure. In Phase I of the project, TNCG verified the presence or absence of security design standards and mitigation recommendations from previous TVAs for facilities and infrastructure under construction. In Phase II of the project, which was just completed, TNCG conducted TVAs for all existing WMATA facilities. TNCG is currently discussing additional scope of work with WMATA.

Contact: Capt. Brian Heanue, Metro Transit Police, (202) 345-0809, BHeanue@wmata.com

Government Client List

AITKIN COUNTY,
Aitkin, Minnesota

ALLAMAKEE COUNTY,
Waukon, Iowa

ASHLAND COUNTY,
Ashland, Wisconsin

AUDUBON COUNTY,
Audubon, Iowa

AUSTIN PUBLIC UTILITIES,
Austin, Minnesota

BARRON COUNTY,
Barron, Wisconsin

BAYFIELD COUNTY,
Washburn, Wisconsin

BEADLE COUNTY,
Huron, South Dakota

BELTRAMI COUNTY,
Bemidji, Minnesota

BENTON COUNTY,
Vinton, Iowa

BLACKHAWK COUNTY,
Waterloo, Iowa

BLUE EARTH COUNTY,
Mankato, Minnesota

BOONE COUNTY,
Belvidere, Illinois

BREMER COUNTY,
Waverly, Iowa

BREVARD COUNTY,
Viera, Florida

BROWN COUNTY,
New Ulm, Minnesota

BUFFALO COUNTY,
Alma, Wisconsin

BUREAU OF CRIMINAL APPREHENSION,
St. Paul, Minnesota

BURNETT COUNTY,
Siren, Wisconsin

BUTLER COUNTY,
Allison, Iowa

CALHOUN COUNTY,
Marshall, Michigan

CAMPBELL COUNTY,
Rustburg, Virginia

CARROLL COUNTY,
Carroll, Iowa

CARVER COUNTY,
Chaska, Minnesota

CASS COUNTY,
Fargo, North Dakota

CASS COUNTY,
Virginia, Illinois

CEDAR COUNTY,
Tipton, Iowa

CHEROKEE COUNTY,
Cherokee, Iowa

CHIPPEWA COUNTY,
Chippewa Falls, Wisconsin

CHISAGO COUNTY,
Center City, Minnesota

CITY AND COUNTY OF LEAVENWORTH,
Leavenworth, Kansas

CITY OF ALBERTVILLE,
Albertville, Minnesota

CITY OF ALLEN,
Allen, Texas

CITY OF ALTOONA,
Altoona, Pennsylvania

CITY OF AMES,
Ames, Iowa

CITY OF ANKENY,
Ankeny, Iowa

CITY OF ANOKA,
Anoka, Minnesota

CITY OF APPLE VALLEY,
Apple Valley, Minnesota

CITY OF ARVADA,
Arvada, Colorado

CITY OF AUSTIN,
Austin, Texas

CITY OF BATTLE CREEK,
Battle Creek, Michigan

CITY OF BELOIT,
Beloit, Wisconsin

CITY OF BISMARCK,
Bismarck, North Dakota

CITY OF BLOOMINGTON,
Bloomington, Minnesota

CITY OF BURNSVILLE,
Burnsville, Minnesota

CITY OF CASPER,
Casper, Wyoming

CITY OF CEDARBURG,
Cedarburg, Wisconsin

CITY OF CEDAR RAPIDS,
Cedar Rapids, Iowa

CITY OF CERES,
Ceres, California

CITY OF CHAMPAIGN,
Champaign, Illinois

CITY OF CHARLOTTE,
Charlotte, North Carolina

CITY OF COLLEGE STATION,
College Station, Texas

CITY OF COLUMBIA HEIGHTS,
Columbia Heights, Minnesota

CITY OF COLUMBUS,
Columbus, Wisconsin

CITY OF COTTAGE GROVE,
Cottage Grove, Minnesota

CITY OF DAYTON,
Dayton, Ohio

CITY OF DECORAH,
Decorah, Iowa

CITY OF DES MOINES,
Des Moines, Iowa

CITY OF DUBUQUE,
Dubuque, Iowa

CITY OF DULUTH,
Duluth, Minnesota

CITY OF DURHAM,
Durham, North Carolina

CITY OF EAGAN,
Eagan, Minnesota

CITY OF EDEN PRAIRIE,
Eden Prairie, Minnesota

CITY OF EDINA,
Edina, Minnesota

CITY OF FARGO,
Fargo, North Dakota

CITY OF FARMINGTON,
Farmington, New Mexico

CITY OF FORNEY,
Forney, Texas

CITY OF FORT ATKINSON,
Fort Atkinson, Wisconsin

CITY OF FORT COLLINS,
Fort Collins, Colorado

CITY OF GAINESVILLE,
Gainesville, Georgia

CITY OF GARLAND,
Garland, Texas

CITY OF GERMANTOWN,
Germantown, Tennessee

CITY OF GOODYEAR,
Goodyear, Arizona

CITY OF GRAND FORKS,
Grand Forks, North Dakota

CITY OF GRESHAM,
Gresham, Oregon

CITY OF GROSSE POINTE FARMS,
Grosse Pointe Farms, Michigan

CITY OF HAM LAKE,
Ham Lake, Minnesota

CITY OF HASTINGS,
Hastings, Minnesota

CITY OF HERMANTOWN,
Hermantown, Minnesota

CITY OF HURST,
Hurst, Texas

CITY OF INVER GROVE HEIGHTS,
Inver Grove Heights, Minnesota

CITY OF IOWA CITY,
Iowa City, Iowa

CITY OF JANESVILLE,
Janesville, Wisconsin

CITY OF KANSAS CITY,
Kansas City, Missouri

CITY OF LINCOLN,
Lincoln, Nebraska

CITY OF MADISON,
Madison, Wisconsin

CITY OF MANKATO,
Mankato, Minnesota

CITY OF MAPLE GROVE,
Maple Grove, Minnesota

City of Maplewood,
Maplewood, Minnesota

City of Marshalltown,
Marshalltown, Iowa

City of McHenry,
McHenry, Illinois

City of Minnetonka,
Minnetonka, Minnesota

City of Minot,
Minot, North Dakota

City of New Hope,
New Hope, Minnesota

City of Nixa,
Nixa, Missouri

City of Oak Grove,
Cedar, Minnesota

City of Oconomowoc,
Oconomowoc, Wisconsin

City of Olivette,
Olivette, Missouri

City of Orono,
Orono, Minnesota

City of Ottumwa,
Ottumwa, Iowa

City of Owatonna,
Owatonna, Minnesota

City of Pingree Grove,
Pingree Grove, Illinois

City of Plymouth,
Plymouth, Minnesota

City of Portland,
Portland, Oregon

City of Raleigh,
Raleigh, North Carolina

City of Richmond Heights,
Richmond Heights, Missouri

City of Robbinsdale,
Robbinsdale, Minnesota

City of Rockford,
Rockford, Illinois

City of Rockwall,
Rockwall, Texas

City of Roseville,
Roseville, Minnesota

City of Round Rock,
Round Rock, Texas

City of St. Cloud,
St. Cloud, Minnesota

City of St. Louis Park,
St. Louis Park, Minnesota

City of St. Paul,
St. Paul, Minnesota

City of Salem,
Salem, Oregon

City of Salina,
Salina, Kansas

City of Santa Cruz,
Santa Cruz, California

City of Savannah,
Savannah, Georgia

City of Seguin,
Seguin, Texas

City of Shoreview,
Shoreview, Minnesota

City of South St. Paul,
South St. Paul, Minnesota

City of Statesboro,
Statesboro, Georgia

City of Superior,
Superior, Wisconsin

City of Tamarac,
Tamarac, Florida

City of Topeka,
Topeka, Kansas

City of Vadnais Heights,
Vadnais Heights, Minnesota

City of Wahpeton,
Wahpeton, North Dakota

City of Watertown,
Watertown, Wisconsin

City of Wausau,
Wausau, Wisconsin

City of Webster Groves,
Webster Groves, Missouri

City of Westland,
Westland, Michigan

City of Williston,
Williston, North Dakota

City of Woodbury,
Woodbury, Minnesota

Clark County,
Neillsville, Wisconsin

Clay County,
Spencer, Iowa

Clay County,
Vermilion, South Dakota

Clayton County,
Elkader, Iowa

Clinton County,
Clinton, Iowa

Codington County,
Watertown, South Dakota

Collin County,
McKinney, Texas

Colorado State Patrol,
Alamosa, Colorado

Columbia County,
Portage, Wisconsin

Convention And Visitors Bureau of Greater Kansas City,
Kansas City, Missouri

Cook Memorial Public Library District,
Libertyville, Illinois

Crawford County,
Prairie Du Chien, Wisconsin

Crow Wing County,
Brainerd, Minnesota

Cumberland County,
Carlisle, Pennsylvania

Dakota County,
Hastings, Minnesota

Dakota County HRA,
Rosemount, Minnesota

DANE COUNTY,
Madison, Wisconsin

DANE COUNTY REGIONAL AIRPORT,
Madison, Wisconsin

DANE COUNTY SOCIAL SERVICES,
Madison, Wisconsin

DAVIS COUNTY,
Bloomfield, Iowa

DECATUR COUNTY,
Leon, Iowa

DELAWARE COUNTY,
Manchester, Iowa

DES MOINES COUNTY,
Burlington, Iowa

DODGE COUNTY,
Juneau, Wisconsin

DODGE COUNTY,
Mantorville, Minnesota

DOOR COUNTY,
Sturgeon Bay, Minnesota

DOUGLAS COUNTY,
Alexandria, Minnesota

DOUGLAS COUNTY,
Douglasville, Georgia

DUBUQUE COUNTY,
Dubuque, Iowa

DUNKLIN COUNTY,
Kennett, Missouri

DUNN COUNTY,
Menomonie, Wisconsin

EASTSIDE SUBURBAN EMERGENCY COMMUNICATIONS CENTER,
Reynoldsburg, Ohio

EAU CLAIRE COUNTY,
Eau Claire, Wisconsin

FAYETTE COUNTY,
West Union, Iowa

FEDERAL RESERVE BANK,
Minneapolis, Minnesota

FOND DU LAC COUNTY,
Fond du Lac, Wisconsin

FOURTH JUDICIAL DISTRICT,
Minneapolis, Minnesota

FRANKLIN COUNTY,
Union, Missouri

FREMONT COUNTY,
Sidney, Iowa

GRAND COUNTY TELEPHONE AUTH. BOARD,
Winter Park, Colorado

GRAND RAPIDS LIBRARY,
Grand Rapids, Minnesota

GRANT COUNTY,
Lancaster, Wisconsin

GREEN LAKE COUNTY,
Green Lake, Wisconsin

GREENE COUNTY,
Springfield, Missouri

GRUNDY COUNTY,
Grundy Center, Iowa

HANCOCK COUNTY,
Carthage, Illinois

HANCOCK COUNTY,
Garner, Iowa

HARDIN COUNTY,
Eldora, Iowa

HENNEPIN COUNTY,
Minneapolis, Minnesota

HO CHUNK NATION TRIBAL JUSTICE CENTER,
Black River Falls, Wisconsin

HOWARD COUNTY,
Cresco, Iowa

IOWA COUNTY,
Dodgeville, Wisconsin

IRON COUNTY,
Hurley, Wisconsin

JACKSON COUNTY,
Black River Falls, Wisconsin

JACKSON COUNTY,
Maquoketa, Iowa

JASPER COUNTY,
Newton, Iowa

JEFFERSON COUNTY,
Fairfield, Iowa

JEFFERSON COUNTY,
Jefferson, Wisconsin

JO DAVIESS COUNTY,
Hanover, Illinois

JOHNSON COUNTY,
Iowa City, Iowa

JONES COUNTY,
Anamosa, Iowa

JUNEAU COUNTY,
Mauston, Wisconsin

KANABEC COUNTY,
Mora, Minnesota

KANE COUNTY,
Geneva, Illinois

KANSAS CITY AREA TRANSPORTATION AUTH. (KCATA),
Kansas City, Missouri

KANSAS CITY POLICE DEPARTMENT,
Kansas City, Missouri

KENOSHA COUNTY,
Kenosha, Wisconsin

KEOKUK COUNTY,
Sigourney, Iowa

KEWAUNEE COUNTY,
Kewaunee, Wisconsin

KIT CARSON COUNTY,
Burlington, Colorado

KNOX COUNTY,
Knoxville, Tennessee

KOOTENAI COUNTY,
Coeur D' Alene, Idaho

LACROSSE COUNTY,
La Crosse, Wisconsin

LAFAYETTE COUNTY,
Darlington, Wisconsin

LAKE COUNTY,
Baldwin, Michigan

Langlade County,
Antigo, Wisconsin

Lee County,
Dixon, Illinois

Lee County,
Fort Madison, Iowa

Lesueur County,
Le Center, Minnesota

Lincoln County,
Merrill, Wisconsin

Linn County,
Cedar Rapids, Iowa

Lisle I-Net Consortium,
Lisle, Illinois

Louisa County,
Wapello, Iowa

Lowell Housing Authority,
Lowell, Massachusetts

Lyon County,
Rock Rapids, Iowa

Manatee County,
Bradenton, Florida

Manitowoc County,
Manitowoc, Wisconsin

Marathon County,
Wausau, Wisconsin

Marquette County,
Montello, Wisconsin

Mayo Civic Center,
Rochester, Minnesota

McDonough County,
Macomb, Illinois

McHenry County,
McHenry, Illinois

McLeod County,
Glencoe, Minnesota

Metropolitan Airports Commission,
St. Paul, Minnesota

Metropolitan Council,
St. Paul, Minnesota

Metropolitan Transit Commission,
Minneapolis, Minnesota

Mille Lacs Driftskippers Snowmobile Club,
Isle, Minnesota

Mills County,
Glenwood, Iowa

Minnehaha County,
Sioux Falls, South Dakota

Minnesota Correctional Facility,
St. Cloud, Minnesota

Minnesota Department of Corrections,
St. Paul, Minnesota

Mitchell County,
Osage, Iowa

Monona County,
Onawa, Iowa

Monroe County,
Tomah, Wisconsin

Morrison County,
Little Falls, Minnesota

Mower County,
Austin, Minnesota

Muscatine County,
West Liberty, Iowa

Northwest Regional Radio Board,
Bemidji, Minnesota

O'Brien County,
Primghar, Iowa

Oconto County,
Oconto, Wisconsin

Orangeburg County,
Orangeburg, South Carolina

Osceola County,
Sibley, Iowa

Outagamie County,
Appleton, Wisconsin

Owatonna Public Utilities,
Owatonna, Minnesota

Ozaukee County,
Port Washington, Wisconsin

Page County,
Clarinda, Iowa

Park County,
Fairplay, Colorado

Pierce County,
Ellsworth, Wisconsin

Pine County,
Pine City, Minnesota

Plymouth County,
Remsen, Iowa

Pocahontas County,
Pocahontas, Iowa

Polk County,
Balsam Lake, Wisconsin

Polk County,
Des Moines, Iowa

Portsmouth Metropolitan Housing Authority,
Portsmouth, Ohio

Poweshiek County,
Montezuma, Iowa

Price County,
Phillips, Wisconsin

Public Building Commission of Chicago,
Chicago, Illinois

Public Housing Agency of the City of Saint Paul,
St. Paul, Minnesota

Ramsey County,
St. Paul, Minnesota

Redwood County,
Redwood Falls, Minnesota

Rice County,
Faribault, Minnesota

Richland County,
Richland Center, Wisconsin

RICHLAND COUNTY,
Wahpeton, North Dakota

RICHMOND HEIGHTS,
Richmond Heights, Missouri

ROBBINSDALE POLICE DEPT.,
Robbinsdale, Minnesota

ROCK COUNTY,
Janesville, Wisconsin

ROCK COUNTY,
Luverne, Minnesota

ROCK RIVER WATER RECLAMATION DISTRICT,
Rockford, Illinois

RUSK COUNTY,
Ladysmith, Wisconsin

SAINT CROIX COUNTY,
Hudson, Wisconsin

SAINT PAUL CIVIC CENTER,
St. Paul, Minnesota

SAINT PAUL PUBLIC LIBRARY,
St. Paul, Minnesota

SAN LUIS VALLEY COUNTY,
Alamosa, Colorado

SANGAMON COUNTY,
Springfield, Illinois

SARPY COUNTY,
Papillion, Nebraska

SAUK COUNTY,
Baraboo, Wisconsin

SAWYER COUNTY,
Hayward, Wisconsin

SEVEN-COUNTY METROPOLITAN PROJECT,
Minneapolis, Minnesota

SHEBOYGAN COUNTY,
Sheboygan, Wisconsin

SHERBURNE COUNTY,
Elk River, Minnesota

SIOUX COUNTY,
Orange City, Iowa

SOUTH DUNKLIN COUNTY,
Hornersville, Missouri

ST. LOUIS COUNTY,
Duluth, Minnesota

STATE OF COLORADO,
Denver, Colorado

STATE OF WISCONSIN,
Madison, Wisconsin

STEARNS COUNTY,
St. Cloud, Minnesota

STEELE COUNTY,
Owatonna, Minnesota

STEVENS COUNTY,
Morris, Minnesota

STODDARD COUNTY,
Dexter, Missouri

STORY COUNTY,
Nevada, Iowa

TAMA COUNTY,
Toledo, Iowa

TAYLOR COUNTY,
Medford, Wisconsin

TOWN OF ADDISON,
Dallas, Texas

TOWN OF GLASTONBURY,
Glastonbury, Connecticut

TRAVERSE COUNTY,
Wheaton, Minnesota

TREMPEALEAU COUNTY,
Whitehall, Wisconsin

VERNON COUNTY,
Viroqua, Wisconsin

VILAS COUNTY,
Eagle River, Wisconsin

VILLAGE OF DEERFIELD,
Deerfield, Illinois

VILLAGE OF GERMANTOWN,
Germantown, Wisconsin

VILLAGE OF GURNEE,
Gurnee, Illinois

VILLAGE OF WESTON,
Weston, Wisconsin

VILLAGE OF WINNETKA,
Winnetka, Illinois

WALWORTH COUNTY,
Elkhorn, Wisconsin

WAPELLO COUNTY,
Ottumwa, Iowa

WARREN COUNTY,
Warrenton, Missouri

WASHBURN COUNTY,
Shell Lake, Wisconsin

WASHINGTON COUNTY,
Blaire, Nebraska

WASHINGTON COUNTY,
Stillwater, Minnesota

WASHINGTON COUNTY,
West Bend, Wisconsin

WAUKESHA COUNTY,
Waukesha, Wisconsin

WAUSHARA COUNTY,
Wautoma, Wisconsin

WEST CENTRAL INTEROPERABILITY ALLIANCE (WCIA),
Wisconsin

WHITE COUNTY,
Carmi, Illinois

WHITESIDE COUNTY,
Morrison, Illinois

WILLIAMS COUNTY,
Williston, North Dakota

WINNEBAGO COUNTY,
Forest City, Iowa

WINNESHIEK COUNTY,
Decorah, Iowa

WINONA COUNTY,
Winona, Minnesota

WISCONSIN, STATE OF,
DEPARTMENT OF REVENUE,
Madison, Wisconsin

WOOD COUNTY,
Wisconsin Rapids, Wisconsin

3. **Provide an estimate of State of Iowa staff time required to complete the Security Assessment.**

   Answer: This will vary depending on the number of facilities assessed. Typically, it will require the State of Iowa to provide a point of contact/manager to work with True North Consulting Group to coordinate building access, interviews with leadership stakeholders, and providing information such as:

   - Listings of key contact personnel
   - Building floor/Open Area Site plans
   - Organizational policies/Written security policies and procedures
   - Description of existing security infrastructure by location/area

   Estimate of State of Iowa time over life of project: Interviews – 1.5 hours per leadership stakeholder
   Project Management - 40 hours

4. **Describe recommended strategy including on-site coordination and support services, best practice consulting options and professional services.**

   Answer: Security Assessments

   Phase I – Physical Security Assessment - Project Initiation

   TASK 1 - Our work would begin with a Project Initiation conference call with the following subtasks:

   a. Introduce TNCG team members and reiterate their roles.
   b. Review the scope of work with DAS and identify the key contact(s) with whom TNCG would work.

   TASK 2- Formulate checklists of needed information and provide those to DAS for completion. Checklists may include requests such as:

   a. Listings of key contact personnel
   b. Building floor/Open Area Site plans
   c. Organizational policies/Written security policies and procedures
   d. Description of existing security infrastructure by location/area

   TASK 3- Review the data and prepare for on-site assessment.

   Phase II – Physical Security Assessment - On-Site Security Assessment

   Upon completion of data collection, TNCG will proceed to conduct on-site security assessments for all locations. The assessment will include observation, data collection, and interviews with necessary staff. The information collected as part of the security systems assessment will be incorporated into the final comprehensive assessment report.

   TASK 4- Work with key personnel to review current policies, procedures, and processes to identify security objectives for DAS.

   a. Assess current readiness/awareness levels and training for staff.
   b. Identify and classify risks.

c. Identify strengths and weaknesses.

d. Define triggers.

e. Analyze gaps.

TASK 5- Conduct interviews and/or focus groups with key stakeholders necessary to clarify, identify, and validate issues and challenges.

TASK 6- Discuss the status/development of policies, procedures, and processes effectiveness of implementation.

a. Review existing emergency/crisis management plans.

b. Review and discuss effectiveness and use of Notification and Warning System.

c. Meet with local law enforcement personnel to discuss security.

d. Review response alternatives

TASK 9- Conduct on-site security assessment for identified areas that will include observation, data collection, and interviews with necessary staff for physical security for:

a. Internal & External

b. Visit sites to examine and document existing conditions, equipment and infrastructure, and determine device locations. Observations are to include:

i. Description of site

ii. Description of the physical properties (gates, fencing, etc.)

iii. Description of the surrounding area (neighborhood, adjacent structures, local businesses)

c. Conduct a review of physical security for facilities and open areas, including supporting infrastructure and equipment, video surveillance, access control, lighting, building entry/exit areas, and other security equipment or systems as applicable.

d. Discuss recent security incidents, and identify threats, risks, and the likelihood of future security incidents based on input from DAS and local law enforcement personnel.

TASK 11 - Present results for staff for comments and feedback on the overall process.

TASK 12 - Conduct assessment of existing network connectivity for security systems.

a. Review communications and security systems and configuration.

b. Assess the capability to handle additional security equipment and integration with the existing network.

c. Provide draft findings and recommendation.

Phase III – Physical Security Assessment - Analysis and Report Development

TASK 13 - Review and discuss:

a. Overall findings from on-site security assessment

b. How existing physical and security technologies and location placement(s) meet DAS requirements

c. Current security systems and/or equipment functionality

d. Video surveillance, video management, access control, lighting systems

e. Content storage and access best practices

f. 'Standards' for future systems expansion and implementation based on locations in building(s), i.e., ingress, egress, halls, stairwells, etc.

g. Building modification needs

TASK 14 - Develop prioritized recommendations based on the information collected, stakeholder interviews, and industry best practices, including:

a. ASIS Protection of Assets Manual

b. FEMA

c. National Crimes Prevention Council

d. National Institute of Justice

TASK 15 - As part of the security systems assessment, provide recommendations to replace, re-purpose, or enhance existing systems.

TASK 16 - Develop budgetary estimates for recommendations for areas of improvement and implementation strategies.

TASK 17 - Develop and deliver a draft Security Assessment Report, including cost estimates for recommendations presented.

TASK 18 - Review report with DAS and then make any modification necessary before submitting the final assessment with cost estimates and next recommended steps.

TASK 19 - Final comprehensive report will include recommended upgrades, gap analysis, migration strategies, timetables, and cost estimates for security technologies.

TASK 20 - (Optional) Present final comprehensive report to DAS management. (TNCG can provide a closed session of findings and an edited findings open session for the public.)

5. **Identify any third-party Respondents involved in Respondent's implementation strategy and describe these relationships.**

   Answer: N/A

6. **Identify the types of deliverables that would be provided as a part of this service.**

   Answer:

   - Progress reports
   - Interview and focus group notes
   - Draft & Final comprehensive report that includes recommended upgrades, gap analysis, migration strategies, timetables, and cost estimates for security technologies.

Exhibit 13 – Security Design Services

1. **Describe Respondent experience with designing Facility Security Systems and Security Management Systems.**

   Answer: True North Consulting Group has extensive experience in providing governmental agencies security design and systems cost estimating. We have been providing security design services throughout our 36 years. We build estimates based on our expert knowledge of market costs for the various elements of security design, including physical security elements, security technology elements, and human resource elements such as security staffing and training. Our cost estimates include initial capital outlay, including hardware, software (if necessary), and installation, as well as ongoing costs such as warranties and maintenance. True North Consulting Group stays actively engaged with product manufacturers, security technology trends, and industry costs.

2. **Describe Respondent experience with designing Access Control, Intrusion Detection and Perimeter Protection Systems.**

   Answer: TNCG stays actively engaged with product manufacturers, security technology trends, and industry costs. Our consultants routinely attend manufacturer training, conferences, and seminars to stay up to date with both existing security systems and new emerging trends.

3. **Describe Respondent experience with designing Digital and Analog Video Security Systems**

   Answer: TNCG's experience with CCTV camera models and video management systems is unparalleled in the industry. We have an in-house camera lab in which we routinely test over 30+ models of cameras as the various manufacturers release them. We share these results received in TNCG's proprietary camera lab (all major manufacturers are tested regularly) with our clients. (For example, two cameras with identical specifications can look and operate very differently.)

4. **Describe recommended strategy including on-site coordination and support services, best practice consulting options and professional services.**

   Answer: ***Design Services***

   TASK 1- Following a security assessment, TNCG will discuss and coordinate with DAS the requirements for specification/standard documents. These specifications/standards will be used for future remodeling projects or new construction at facility sites as needed. The specifications/standards will include (but may not be limited to):

   a. Security Protocols
   b. Entry/Exit Areas
   c. Video Surveillance, Monitoring, and Storage
   d. Access Control
   e. Intrusion Detection
   f. Lock and Key Control
   g. Alarm Systems
   h. Lighting (TNCG will provide standards limited to lighting levels and general lighting technology (LED).)

TASK 2- Produce detailed design drawings, including:

a. Device locations
b. Schedules showing individual make, model, mounting conditions, and other notes
c. Installation details and connectivity diagrams.

TASK 3- Develop draft security specifications/standards that include security protocols, entry/exit areas, lighting, video surveillance, video management, access control, and alarm systems. These specifications/standards will be used for future remodeling projects or new construction at treatment facility site. The specifications include:

a. "Front-end" document including
    i. Information for potential proposers/bidders
        1. Important dates/timeline
        2. Scope of the Project
        3. Information about Pre-proposal/Pre-bid meeting and Addenda
        4. Evaluation criteria
    ii. Submission/response requirements
    iii. Discuss and determine vendor qualification requirements
    iv. Terms and conditions (including Agreement form)
b. TNCG will create the Technical Specifications portion(s) of the document to include:
    i. General/background information about the project
    ii. Instructions for submittals required at the time of proposal and the format in which those are to be supplied
    iii. Overall/general technical requirements
    iv. Delivery requirements
    v. Description of materials required (with quantities where appropriate), including brand names to establish equivalency requirements (as needed)
    vi. Specific instructions for installation of systems
    vii. Testing and acceptance criteria
    viii. Documentation requirements
    ix. Proposal/bid form with items for respondents to fill in *(including qualifications and pricing information)*
    x. Proposal bond form to be submitted with the response
    xi. Sample Performance and Payment bond forms
    xii. Sample Application for Payment forms

TASK 4- Review draft security specifications/standards with DAS and incorporate edits and comments.

TASK 5- Deliver final security specifications/standards to DAS.

TASK 6- Conduct Project Meetings and Coordination, including:

a. **Kick-Off Meeting**: TNCG will chair an initial project meeting to review known expectations and design concepts. The purpose of the meeting is to discuss schedules and implementation strategy expectations, agree on the document requirements document, and agree on the level of detail required on all updated documents.

b. **60% Progress Meeting**: A second discussion will be scheduled to review the 60% drafts of all documents and receive feedback from DAS for inclusion in the final deliverables. The primary focus of this meeting is to review the draft documents format, structure, table of contents, and for DAS to provide feedback on key items prior to completion of the documents.

c. **95% Document Review Meeting**: TNCG will coordinate and present the 95% complete specifications/standards document to DAS. All outstanding feedback will be discussed at this meeting for inclusion in the final documents.

d. **Security Specifications**: TNCG will create security guideline specifications in Division 27 CSI MasterFormat. Specifications will include general product and execution requirements. These documents are intended to be incorporated (with project-specific edits) in future project Construction Documents (CDs).

e. **Project Completion**: At the conclusion of the project, TNCG will provide the completed Specifications/standards document and diagrams/detail drawings for each system in electronic format and deliver to DAS.

5. **Provide an estimate of State of Iowa staff time required to complete the Security System Design, if different than Exhibit 11.**

   Answer: This will vary depending on the design of the system/project. Typically, it will require the State of Iowa to provide a point of contact/manager to work with True North Consulting Group during the coordination of design, interviews, review of design, and implementation of system design.

   Estimate of State of Iowa time over life of project: Interviews – 1.5 hours per stakeholder

   Project Management - 20 hours

6. **Describe recommended strategy including on-site coordination and support services, best practice consulting options and professional services, if different than Exhibit 11.**

   Answer: N/A - Duplicate

7. **Identify any third-party Respondents involved in Respondent's implementation strategy and describe these relationships, if different than Exhibit 11.**

   Answer: None

8. **Identify the types of deliverables that would be provided as a part of this service.**

   Answer:

   - Schematic Design options
   - Cost estimates
   - Detailed design drawings including device locations, schedules showing individual make, model, mounting conditions, and installation details and connectivity diagrams
   - Specifications

Exhibit 14 – Sample Reports

Please see True North's sample reports on the following pages.

REDACTED High School

Security Risk Assessment

October 16, 2018

True North Consulting Group
3408 Hillcrest Drive
Waco, Texas 76643

Contents

EXECUTIVE SUMMARY 4

BACKGROUND 6

ASSETS AND CONSEQUENCES 8

THREAT ASSESSMENT 11

FINDINGS AND RECOMMENDATIONS 22

VULNERABILITY ANALYSIS 43

RISK ASSESSMENT ANALYSIS 45

PROTECTIVE MEASURES SUMMARY AND PRIORITIZATION 48

CONCLUSION 52

APPENDIX I: CRIMECAST® REPORT 53

APPENDIX II: GLOSSARY OF COMMON TERMS 55

-DISCLAIMER-

This report is issued by True North Consulting Group (TNCG) to [redacted] High School for its own use. No responsibility is accepted for any other use of this report for any other purpose or by third parties. This report contains the opinion of TNCG regarding security threats as they relate to the current preparedness of the school in the mitigation of such threats. This report was prepared in 2018 using information available to TNCG and its consultants at that time. TNCG accepts no responsibility for subsequent changes, errors, or omissions in relation to material quoted in the report. Implementation of security measures based on the observations contained in this report does not guarantee the prevention of a terrorist attack or a criminal act against the school, its assets, or its stakeholders.

Executive Summary

In August 2018, True North Consulting Group (TNCG) conducted a Security Risk Assessment (SRA) of [redacted] with the objectives to: 1) assess the school's current state of preparedness for dealing with manmade threats, 2) identify gaps where security measures fall short and provide associate recommendations, and 3) ensure adherence to state security and emergency response legislation, regulations, guidelines, standards, and best practices.

Given the current threat environment, malicious acts against school assets may be carried out by both internal and external actors. The school must seriously consider threats posed by idiosyncratic, criminal, or ideologically motivated actors who may commit shooting, assault, vandalism, theft, burglary, arson, or vehicle ramming against the organization and its assets.

TNCG noted several deficiencies in the school's current physical, technological, and human security posture and emergency preparedness. These gaps increase the exposure of the district's facilities and their occupants to the above listed Potential Methods of Attack (PMAs).

The main areas where vulnerabilities and security gaps exist are the following:

- Security Staffing: Security deployment is not strong enough to prevent or respond to security incidents. [redacted] has only one SRO and two security guards. The school serves over 2,200 students and it is recommended that more SRO's are staffed here. Furthermore, at least one officer (district or law enforcement) should be present at all times the building is occupied.
- Exterior Property Security Detection and Access Control. The school cannot physically restrict pedestrian or vehicle access to most sections of the property. [redacted] also lacks sufficient measures such as surveillance, lighting, and emergency intercoms to detect and respond to criminal activity. Installation of high-quality perimeter fencing, blue-light call boxes, additional high-quality cameras, and securable vehicle gates will improve the overall security of the property.
- Layout & Design: The school is currently set-up in a fashion that leaves students vulnerable to crime from trespassers. Several of the buildings are void of access controls and left unlocked. This occurs while the students are walking between buildings in broad daylight without the security of a protected hallway. Installing RFID readers to these buildings along with an app on the students' smartphones will provide the students a safer way of getting to class.
- Security Culture: There is currently no training of students or staff regarding emergency preparedness. They have not undergone drills or "red-team" activities that prepare them for what will occur during a security event. Drills throughout the school year will provide all those inside the school with the knowledge of how to react.

[redacted] should recognize that there is no silver bullet application capable of providing foolproof security protection. However, the recommendations presented in this report can place the school in a superior position to safeguard people and other critical assets.

Background

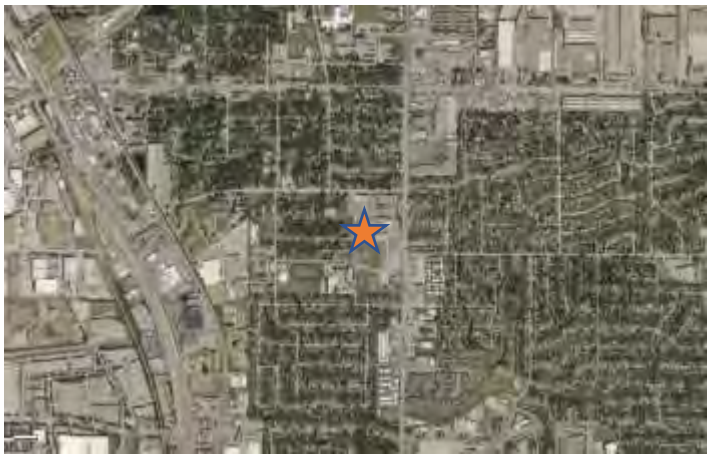
Overview

[redacted] High School ([redacted]) is located in [redacted], [redacted]. The school provides educational and extra-curricular activities to students in 9th-12th grades in the northern suburbs of [redacted], [redacted].

The threats and vulnerabilities listed below are applicable to [redacted] and the functions performed within the school. The mitigation and recommendations provided do not guarantee an attack will not happen; however, they can dramatically decrease the possibility of the facility being chosen as a target, interrupt a plan of attack, slow down an attack to minimize damage, improve the response in the event of an attack, and assist in gathering evidence should an attack occur.

Location

[redacted] is located at [redacted], [redacted]. Residential, commercial, and educational properties are in proximity to the [redacted] campus.



Vicinity Map

Site Layout

1. Access roads from [redacted] Road, and [redacted] Road.
2. Constructed in 1960, the school consists of 8 buildings, some including multiple floors.
3. The 20 exterior doors provide direct access to the building. Additionally, there is one set of vehicle bay doors. Public access to the building occurs at one location near the corner of [redacted] Lane and [redacted] Road.

General Operations

1. The primary function is to serve as an educational and social environment for teenagers.
2. Most administrative offices are located on the Northeast side of the building.
3. During non-school days, most access to the school is for the purpose of athletic events.
4. Receiving of food for the cafeteria and kitchen occurs on the West side of the property in the loading dock area.
5. Special events include the [redacted] County Promise Tailgate Kick-off which show students from the high schools in the district how to take advantage of free college tuition at [redacted] Community Colleges. Another special event is the Parenting the Love & Logic Way seminar which teaches parents necessary skills for handling difficult situations with their children.
6. After-school activities include a myriad of athletics such as baseball and soccer and classes for those interested in cosmetology.

Hours of Operation

1. Normal school hours are 08:20-15:35 Monday through Friday.
2. The building opens at 06:30 and closes at 23:30 Monday through Friday.
3. Typical delivery hours are 08:00-15:00 Monday through Friday.
4. Weekend hours vary due to the scheduling of athletics and extra-curricular activities.

Occupants

Regular facility occupants include:

1. Students. Total enrollment for [redacted] is 2,033.
2. Parents and family members.
3. Teachers.
4. Administrative staff.
5. Janitorial and custodial staff.

Assets and Consequences

Assets are those components that are integral to an organization's operations and reputation. From a security perspective, assets are what must be protected against loss. The value of an asset to an organization may range from very high to very low depending on several factors including:

- Criticality of the asset to the organization's operations and / or reputation.
- The ability of the organization to function without the asset.
- The redundancy of the asset within the organization.
- The resources necessary (time, money, etc.) for the organization to recover if lost.

The scope and focus of this security assessment are to identify security gaps that may result in increased vulnerabilities related to the most critical and important assets. During the onsite interview, TNCG consultants and school personnel identified high-value assets which, if lost, would have varying levels of impact on the organization.

The following list describes and ranks the top assets of each school that, if lost, would cause the facility to suffer from negligible to exceptionally grave consequences.

Asset Value Table

The scope and focus of this security assessment is to identify security gaps that may result in increased vulnerabilities related to the most critical and important assets as identified by the school and TNCG consultants. The following table and legend explains the value criteria used to assess the criticality of each asset.

Asset Value	
Very High	10
High	8-9
Medium-High	7
Medium	5-6
Medium-Low	4
Low	2-3
Very Low	1

Asset Value Table

- Very High – Loss or damage to assets would have exceptionally grave consequences such as extensive loss of life, widespread severe injuries, or total loss of primary services and core functions and processes. The consequences would have an exceptionally grave effect on public health and safety, the economy, and governance.
- High – Loss or damage of school assets would have grave consequences such as loss of life, severe injuries, loss of primary services, or major loss of core functions and processes for an extended period. The consequences would have a grave effect on public health and safety, the economy, and governance.
- Medium High – Loss or damage of assets would have major consequences such as severe injuries or impairment of core functions and processes for an extended period. The consequences would have a serious effect on public health and safety, the economy, and governance.
- Medium – Loss or damage of assets would have moderate to serious consequences such as injuries or impairment of core functions and processes. The consequences would have a moderate to the serious effect on public health and safety, the economy, and governance.
- Medium Low – Loss or damage of assets would have moderate consequences such as minor injuries or minor impairment of core functions and processes. The consequences would have a moderate effect on public health and safety, the economy, and governance.
- Low – Loss or damage of assets would have minor consequences such as a slight impact on core functions and processes for a short period. The consequences would have a minor effect on public health and safety, the economy, and governance.
- Very Low – Loss or damage of site assets would have negligible consequences or impact.

High-Value Assets

During the assessment, TNCG consultants and school personnel identified the following high-value assets which, if lost, would have varying levels of impact on the organization.

Asset	Value	Numeric Value	Description/Location
People	Very High	10	Students, staff (administrative, teaching, support, maintenance), volunteers, visitors.
Building	High	9	Core setting for educational activities. In most cases, the current CoOP plan does not outline long term continuity of services if the building is lost.
Data and Telecom Infrastructure	High	9	Servers and network switches. Facilitates connectivity both within and across schools.
Student Medication	High	8	Regularly administered for chronic conditions.
Exterior Utilities	Medium-High	7	Electricity, water, natural gas, HVAC. Emergency generators are not present at any school.
Interior Utilities	Medium-High	7	Control infrastructure for electricity, water, natural gas, HVAC.
Specialty Equipment	Medium	5	AV equipment, computers, special needs equipment.
Sensitive Documents	Medium	5	Student/employee records and information.
Cash/Checks	Very Low	1	Cash on Hand (less than $10,000)
Outside Facilities (Athletic)	Very Low	1	Baseball field, tennis courts, track & field stadium, and football field.

Assets Identification and Prioritization Table

Threat Assessment

Overview

The objective of this threat assessment is to provide a global and historical context for potential threat elements (PTEs) as well as provide a study of their motivations and capabilities. This section will provide data and insights on similar plots, incidents, actors, targeting rationales, and methods involving attacks on other schools.

In order to gain a clearer perspective on the rate at which school shootings occur in the United States, it is beneficial to take a global approach.

In May 2018, CNN conducted an analysis of school shootings in the U.S. compared to other countries with the largest advanced economies in the world. These incidents were from January 1, 2001 through May 21, 2018 and had to involve at least one injury. According to their research at the time, there had been *at least* 288 school shootings in the U.S. since January 1, 2009; this equates to 57 times as many incidents as the other six countries in the study.[1]

Target Profile

The overarching target characteristics associated with the school and occupants are those of an educational institution. The following components comprise the overall target profile. Threat actors may regard specific elements or combinations of elements as potentially attractive targets.

- Interior facility:
  - Entrances.
  - Emergency and non-emergency exits.
  - Loading areas.
  - Classrooms.
  - Offices.
  - Computer/specialty equipment.
  - Hallways.
  - Locks.

- Exterior facility:
  - Parking.
  - Building proximity.
  - Athletic fields/courts
  - Trash/waste bins.
  - Locks.

- Occupants:
  - Students.
  - Students' families.
  - Teachers.

[1] https://www.cnn.com/2018/05/21/us/school-shooting-us-versus-world-trnd/index.html

  - Staff.
  - Administrative personnel.
  - Visitors.

- Utilities:
  - Electrical.
  - HVAC.
  - Water/sewage system.
  - Internet/telecommunications.

- Events:
  - Athletics.
  - Plays.
  - Community gatherings.
  - Beginning/end of school-year celebrations or ceremonies.

Incidents Occurring at [redacted] High School

During the onsite assessment, interviewees referenced the following potential threats:

- In 2017, there was a shooting in the neighborhood behind the school. [redacted] students were involved, and the school initiated lockdown procedures.
- On 1/28/2013, a student was dared by a friend to call in a bomb threat. He was identified and expelled.
- In Spring 2017, a student wrote threatening messages on the school bathroom wall saying, "Shooting tomorrow at noon". After interviewing the student, it was determined that the student's motive was primarily to disrupt the school, not to act violently.

Recent Major School Attacks (2010-2018)

A number of violent attacks, plots, and attempted suicides in school environments in recent years, perpetrated by students, teachers, staff, and individuals unaffiliated with the particular school, has underscored the threat of idiosyncratic motives violence at schools and universities.

- May 18, 2018 // Santa Fe, Texas—At 07:40, police began receiving calls of shots fired at Santa Fe High School. Dimitrios Pagourtzis, a 17-year-old student at the school, began his shooting spree in an art class. By the end, 10 people were killed and 13 were injured. Investigators later revealed that Pagourtzis had intended to commit suicide, but after a shootout with police, decided to surrender. He is being held in jail on a capitol murder charge, without bond.[2]
- February 14, 2018 // Parkland, Florida—Shortly before school dismissal, 19-year-old Nikolas Cruz, a former student, opened fire at Marjory Stoneman Douglas High School. Cruz had been expelled previously from the school for disciplinary reasons and has reportedly posted on YouTube, "I'm going to be a professional school

[2] http://www.businessinsider.com/santa-fe-shooter-police-gunfire-15-minutes-2018-5

shooter." Using a semi-automatic rifle, Cruz killed 17 and wounded 14. Authorities announced Cruz's capture by 16:00 the same afternoon. [3]

- December 15, 2015 // Los Angeles County, California—The Los Angeles County shut down all of its schools after receiving a credible terrorist threat that turned out to be a hoax. Los Angeles County has 900 schools and 187 public charter schools, and over 640,000 students.[4]
- October 3, 2015 // Tuolumne, California—Four high school students were arrested for planning a shooting attack on Summerville High School. Police discovered evidence of detailed plans, names of targets, locations, and methods the attackers would use during the attack. The suspects were still in the process of acquiring weapons.[5]
- October 1, 2015 // Roseburg, Oregon—At 10:38, Chris Harper-Mercer (age 26) opened fire on the Umpqua Community College campus. After eight minutes, police neutralized the shooter, but there were nine fatalities and 20 injured.[6]
- October 24, 2014 // Marysville, Washington—At approximately 10:39, Jaylen Fryberg, a student at Marysville Pilchuck High School, opened fire inside the school cafeteria, killing four students and wounding another before turning the gun on himself and committing suicide.[7]
- April 21, 2014 // Griffith, Indiana—Remanard Castro, aged 55, shot his estranged wife, Nina, in the parking lot of St. Mary's Catholic School. The shooting occurred at approximately 16:30 as Nina and her 16-year-old daughter were collecting her 14-year-old son from school. Castro later committed suicide at his home after being confronted by police.[8]
- June 7, 2013 // Santa Monica, California—Six died and four were injured in a shooting at Santa Monica College. The gunman, John Zawahri, killed his father and brother before going to the campus library and opening fire. The shooter was killed by responding police officers.[9]
- December 14, 2012 // Newtown, Connecticut—Adam Lanza, 20, killed his mother at his home, and then traveled to Sandy Hook Elementary School where he shot and killed 20 children and six adults before committing suicide.[10]
- March 6, 2012 // Jacksonville, Florida—After being fired from a teaching position earlier in the day, Shane Schumerth returned to the school with an AK-47 in a guitar

[3] https://www.nbcnews.com/news/us-news/police-respond-shooting-parkland-florida-high-school-n848101
[4] http://www.motherjones.com/mojo/2015/12/los-angeles-county-shuts-down-all-schools-due-credible-terrorist-threat
[5] http://www.usatoday.com/story/news/nation/2015/10/04/students-arrested-shooting-plot/73325610/
[6] https://www.washingtonpost.com/news/morning-mix/wp/2015/10/02/oregon-shooter-said-to-have-singled-out-christians-for-killing-in-horrific-act-of-cowardice/?1234123
[7] http://www.theindychannel.com/news/local-news/1-dead-in-shooting-at-nw-ind-school-parking-lot
[8] http://www.nbcchicago.com/news/local/Man-Shoots-Estranged-Wife-in-School-Parking-Lot-256119341.html
[9] http://www.cnn.com/2013/06/07/us/california-college-gunman/index.html?hpt=hp_t2
[10] http://www.cnn.com/interactive/2012/12/us/sandy-hook-timeline/index.html

case, entered the head of school's office, shot her multiple times, and then turned the gun on himself.[11]

- October 8, 2010 // Carlsbad, California—Brendan Liam O'Rourke, 41, shot at a group of elementary school children with a .357 handgun, injuring two girls, ages 6 and 7. O'Rourke wanted to target wealthy children with his attack. He received a life sentence for his crimes.[12]

Threat Actor Motivations

The following are key threat actor motivations that are relevant to K-12 schools. TNCG has divided these motivations into four distinct categories:

A. Idiosyncratic Motives Threat Actors

Individuals driven by idiosyncratic motives represent a serious threat to school assets. This actor may carry out violent attacks against school employees and students. Rather than being driven by financial or material gain, this PTE's motive will most likely be related to a range of personal factors and events including: serious mental illness and emotional instability; workplace grievances and dynamics such as the loss of a job or termination; feelings of acute alienation, humiliation, rejection, and/or revenge; domestic disputes; personal life shocks or hardships such as the end of a significant relationship, legal issues, and/or financial strain; and, personal biases and grudges. Four types of idiosyncratic motives attackers should be considered as primary threats to the school's target profile:

1. Workplace conflicts resulting in violence, sabotage, or theft of sensitive materials.
2. Domestic/partner abuse and violence.
3. Disgruntled students, staff, or family members.
4. Mental health and other motives.

Targeting/Attack Objectives	Plausible Potential Methods of Action (PMAs)
• Cause mass casualties. • Kill/injure students. • Kill/injure staff member(s). • Kill/injure family member(s). • Damage/destroy product and infrastructure.	• Shootings. • Manual/physical attacks (punches, kicks, and bladed or blunt hand-held weapons). • Vehicle ramming. • Sabotage. • Arson/Improvised Incendiary Device (IID). • Improvised Explosive Devices (IEDs).

B. Criminally-Motivated Threat Actors

The criminally-motivated PTE represents the most relevant threat to the school's physical assets. This PTE is usually driven by the desire for personal material gain

[11] http://jacksonville.com/news/crime/2012-03-06/story/episcopal-school-head-dale-regan-killed-fired-teacher-who-then-kills
[12] http://www.cbsnews.com/news/carlsbad-calif-school-shooter-gets-189-years-to-life/

rather than by ideology. Additionally, this PTE may operate as an individual or as part of a larger group.

Although incidents carried out by criminal perpetrators are far more common when compared to idiosyncratic- or bias-motivated incidents, they are generally focused on material gain and are therefore less likely to result in mass casualties. It should be noted that this PTE may work with or employ PMAs utilized by ideologically-motivated PTEs. However, the criminally motivated PTE's ultimate goal will remain personal material gain.

Targeting/Attack Objectives	Plausible Potential Methods of Action (PMAs)
• Personal financial/material gain.	• Theft of cash or other materials with significant monetary value. • Destruction of property. • Vandalism. • Arson/Improvised Incendiary Device (IID). • Sabotage. • Cyber Intrusion/Hacking.

Criminal acts surveyed by TNCG are divided into two operational categories and two motivational categories. The operational categories are:

1. Violent Crimes – Crimes affecting the physical wellbeing of the victim. These crimes include homicide, sexual assault, robbery, and aggravated assault.

2. Property Crimes – Crimes involving unlawful access to or destruction of intellectual or physical property. These crimes include burglary, theft, motor vehicle theft, and arson.

The motivational categories for crime are:

1. Criminal activity for personal benefit and profit.
2. Gang activity and organized crime.

Location Risk Forecast

Background

A CRIMECAST® report from CAP Index, Inc. has been obtained for this location. This report, which provides data and information pertaining to local crime in the area, assists in establishing a level of risk at [redacted] properties. The CRIMECAST® model is based upon the relationship between a neighborhood's "social disorder" and the amount of crime perpetrated there.

The key deliverable of this report is a set of site scores which reflect a site's risk by comparing the location's relative "social disorder" to the national and state averages. Relative threat level scores for this report are determined by assessing areas within a one and three-mile radius, or on population density thresholds of

25,000 and 100,000 people, respectively. The score is the outcome of the comparison between the two radii.

Scores range between 0 and 2000, and a score of 100 represents the average level. A score above 100 means that this location is proportionately more likely to be subject to crime as it relates to a specific level. For example, a score of 250 at the National CAP Index means that this location has a 2.5 times higher likelihood of a crime occurring there than the national average when comparing this site to every addressable location in the United States.

[redacted] High School Cap Index Score

[redacted] High School has an overall National Current Cap Index score of 155. This score means that there is a relatively high risk of a criminal incident occurring at or near this site. For a more comprehensive dataset and an in-depth analysis of the CRIMECAST® report, please see Appendix I.

C. Hate/Bias-Motivated Threat Actors

TNCG assesses the threat of hate- or bias-motivated violence against school facilities to be relatively low. The school populations do not represent a distinct racial, ethnic, or socio-economic group that would be particularly targeted by such extremist groups. However, certain right-wing groups may consider public city-run schools to be representative of the "enemy" (i.e. government).

It should be noted that there is a high amount of overlap between bias-motivated and idiosyncratic-motivated PTEs in terms of likely or plausible PMAs. This is because while the motives may be different, the desired outcome is often similar.

Targeting/Attack Objectives	Plausible Potential Methods of Action (PMAs)
• Cause mass casualties. • Kill/injure individuals of a specific race, ethnicity, religion, or sexual orientation. • Interrupt operations/cause financial damage. • Damage/destroy equipment and infrastructure.	• Shootings. • Manual/physical attacks (punches, kicks, and bladed or blunt hand-held weapons). • Vehicle ramming. • Vandalism. • Sabotage. • Arson/Improvised Incendiary Device (IID). • Improvised Explosive Devices (IEDs). • Protests/Intimidation.

D. Islamist Terrorism and Homegrown Violent Extremism (HVE)

Although Islamist Terrorists and HVEs likely represent a low threat to the school, the threat still requires serious attention. Islamist terrorists have frequently targeted school environments overseas, as evidenced by attacks in Pakistan by the Pakistani Taliban, and in Nigeria by Boko Haram.[13]

One of the most well-known terrorist attacks on a school occurred on September 1, 2004, when approximately 30 members of a Chechen Separatist-Islamist terrorist organization seized a school in Beslan, Russia. The attackers took approximately 1200 students, teachers, and parents hostage, corralling them in the school gymnasium. By the end of the three-day siege – which included bomb explosions in the gymnasium and a chaotic battle between the terrorists and Russian forces – approximately 344 people had been killed, including 186 children, with 727 wounded.

In another prominent attack, Mohammed Merah, a 23-year old French citizen of Algerian origin, conducted three shooting attacks targeting military personnel and a Jewish school in the Toulouse area on March 19, 2012. He killed seven and wounded two. According to reports, Merah approached the Ozar Hatorah Jewish School in Toulouse on a scooter and opened fire in the schoolyard, killing three

[13] http://www.csmonitor.com/USA/Foreign-Policy/2014/1216/Pakistan-school-attack-Why-children-are-becoming-a-more-common-terror-target

children and a teacher and wounding another student. Merah claimed to be a member of Al Qaeda and conducted the attacks to protest the French military presence in Afghanistan and "the killing of Palestinian children." Reports suggest that Merah acted without direction from Al Qaeda or affiliated groups, and that the Jewish school was a spur-of-the-moment alternate target after Merah was unable to locate his intended primary target, another member of the military.

To date, schools inside the United States have not been featured prominently on the list of desired targets for overseas terrorist organizations. However, this situation could change as a result of one or both of the following factors:

Recruitment—The recent surge in attempts by U.S. residents to travel overseas to join al-Shabab, ISIS, and other organizations demonstrates that Islamist militant sentiment does exist locally. As efforts to prevent potential recruits from flying overseas become more successful, such recruits may become increasingly frustrated and look to attack different high-profile targets within the U.S. A successful attack against a school would most likely create the desired publicity and psychological trauma.

Evolving Conflict—As past propaganda has demonstrated, foreign Islamist groups have continued to modify and expand their target list as the conflict with the United States continues. Recent calls by groups such as ISIS for HVEs to target members of the military, law enforcement, and emergency services demonstrate that successful attacks against the U.S. no longer depend on the attacker receiving training and guidance overseas. As the conflict between the U.S. and foreign Islamist groups continues to evolve, it is highly possible, if not imminent, that these groups will start openly calling for attacks against schools within the U.S.

Threat Actors' Origins

In addition to motivation, PTEs may be divided into two general categories based on their relationship to the school:

A. Internal Actors

Internal actors, those individuals who are considered regular members of the school, represent a serious threat to the organization because many of them have relatively easy access to the facilities' and organization's highest-value assets such as occupants and high-value materials. Based on the school's operational classifications, the following groups should be considered as potential internal actors:

- Students.
- Faculty.
- Long-term contracted staff such as janitors.
- Family members.

B. External Actors

External actors are individuals not regularly associated with the school community. The amount of pre-operational preparation required for external actors is generally much higher, increasing the potential for early detection and neutralization of threats. Furthermore, external actors are more likely to disguise themselves as individuals with approved access to sensitive areas. This may be done using falsified identification or credentials or by pretending to be emergency responders. External actors may include the following:

- Delivery personnel.
- Former employees or acquaintances of current employees.
- Acquaintances of students.
- Members of the general public.

It is important to note both internal and external actors may be driven by criminal, idiosyncratic, or political/religious ideological motives.

PMA Threat Analysis Overview

To numerically evaluate and rank primary threats to the school, this assessment utilizes the criteria provided below. It is important to note that this analysis does not reflect any of the existing protective measures currently deployed; rather the intent behind this analysis is to highlight and rank the threat probability to the school. Scores from one to 10, with one being the lowest and 10 being the greatest threat, are assigned based on the following criteria:

i. Access to Weapon

This refers to the ease by which the source material can be acquired to carry out the attack. Consideration includes local materials from HazMat inventories, farm and mining supplies, major chemical or manufacturing plants, university and commercial laboratories, and known contraband sources and transportation centers. The score range in this category is as follows:

0 – Complex to obtain in the region.
1 – Possible to obtain but corroboration with additional providers is required.
2 – Easy to obtain in the region but a risk of being suspected exists.
3 – Easy to obtain in the region with minimal risk of being suspected.

ii. Knowledge/Expertise

The general level of skill and training combines the ability to create the weapon (or arm an agent) and the technical knowledge of the systems to be attacked (e.g. heating, ventilation, and air conditioning [HVAC], nuclear, etc.). Knowledge and expertise can be gained by surveillance, open source research, specialized training, or years of practice in the industry. The score range in this category is as follows:

0 – Complex; high level of training is required.
1 – Easy; minimal level of knowledge is required, and information is readily available.

iii. Targeting
Has the protected environment been subject to this threat before? When was the most recent incident and where, and against what target? Are the specific building's functions and occupants an attractive target for the potential threat elements? The score range in this category is as follows:

0 – The protected environment has never been a subject to this threat.
1 – The protected environment has never been a subject to this threat but other facilities/organizations with a similar target profile in the region have been targeted within the past two years.
2 – The protected environment has been a subject to this or a very similar PMA within the last two years.

iv. Asset/Target Profile/Attractiveness
The protected environment has varying levels of symbolic and economic importance to both the targeted entity and the PTE. The protected environment has significant high-value assets. The score range in this category is as follows:

0 – No symbolic, economic, or strategic value to the targeted entity or PTE and no high-value assets are present onsite.
1 – The protected environment has a number of high-value assets that could be easily transformed in currency or if damaged will somewhat correspond with the motive of the PTE.
2 – The protected environment has a high number of high-value assets onsite as well as strategic and/or economic importance for the PTE.
3 – The protected environment has symbolic, economic, and strategic importance to the targeted entity or a number of extremely high-value assets that will perfectly correspond with the motive of the PTE.

v. Site Population/Capacity/Impact
The population demographics and potential number of people directly impacted by this PMA. The score range in this category is as follows:

0 – Low populace deters or is not a pivotal factor for this PMA.
1 – High populace attracts or is a pivotal factor for this PMA.

PMA Threat Assessment Table

Potential Methods of Action	Access to Weapon	Knowledge	Targeting	Target Profile	Site Population	Score & Rank
Values	0-3	0-1	0-2	0-3	0-1	0-10
Shooting	3	1	2	3	1	10
Assault	3	1	2	2	0	8
Vandalism	3	1	2	1	0	7
Theft	3	1	2	1	0	7
Burglary	3	1	0	1	0	5
Arson	3	1	0	1	0	5
Vehicle Ramming	3	1	0	1	1	6
Improvised Explosive Device	2	1	1	1	1	6
Sabotage	3	1	0	1	0	5
Car Bomb	2	0	0	1	1	4
Chemical/Biological Weapon	1	0	0	1	1	3
Mail/Package Device	1	0	0	1	0	2

This threat analysis illustrates an assessment of aggressors' PMAs against school facilities and high-value assets. It is important to note that this analysis does not reflect any of the existing protective measures; rather the intent behind this analysis is to highlight and rank the threat probability and threat probability only. Based on our findings, we believe the following aggressors' PMAs pose the highest threat to its most critical assets:

1. Shooting.
2. Assault.
3. Vandalism.
4. Theft.

Findings and Recommendations

The table below includes vulnerabilities and subsequent recommendations that were identified by the pre-assessment and during the onsite visit and interviews. Each of the listed items includes a description (with or without visual) of the threat and vulnerability, as well as the recommended corrective actions.

The protective value of the recommended corrective actions regarding their ability to reduce overall organizational risk can be found below in *Protective Measures Summary and Prioritization—Protective Measures Prioritization Guideline*.

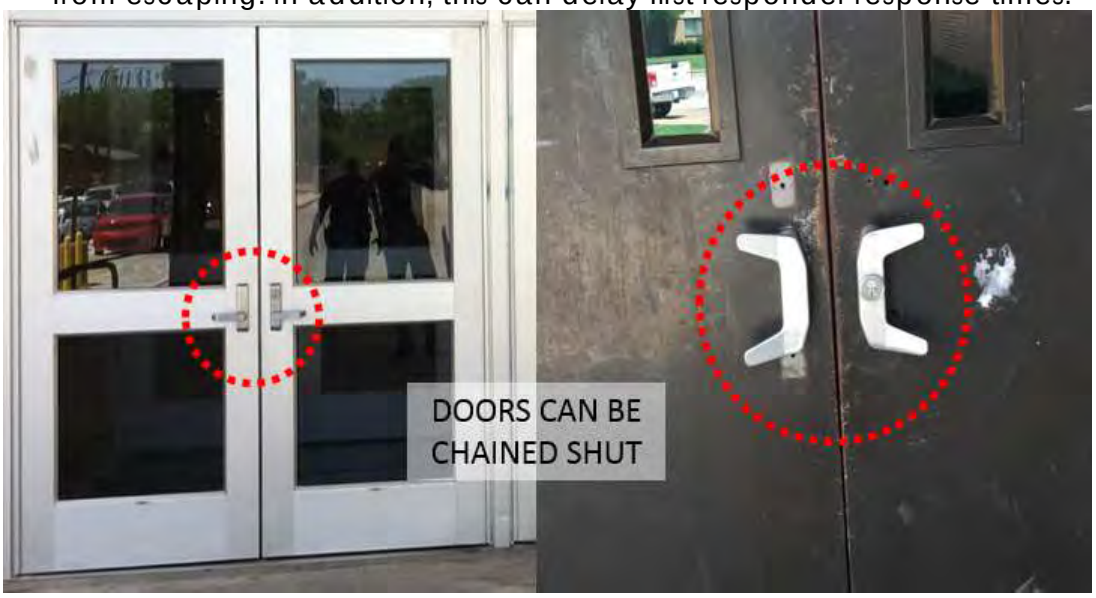
1	Threats and Vulnerabilities	<u>Exterior Detection</u>
		School is currently unable to deter, detect, or prevent unauthorized pedestrian or vehicle access onto the properties. This exposes the school to the following potential threat scenarios:
		• During normal school operations:
		  o Violent PMAs such as assault, shooting, or kidnapping targeting individuals or groups of students or staff located inside or outside the school building.
		• Outside normal operations:
		  o Violent PMAs such as assault, shooting, or kidnapping targeting individuals, primarily staff members, located on the school property.
		  o PMA's such as vandalism, burglary, theft, and arson targeting schools' physical assets.
		  o These PMAs are more likely to occur at lowlight locations and times.
		Contributing deficiencies included the following:
		• Insufficient exterior security camera coverage aside from building-mounted camera hovering visitors.
		• Insufficient lighting at perimeter parking areas. Quality is inadequate and the energy management system automatically turns off lights daily at midnight to save energy costs. This is a liability as the school is occupied for roughly twenty-two hours of the day.
		• No emergency intercoms anywhere in the parking areas. These boxes alert law enforcement when an individual is in immediate danger. Students and staff should be properly trained on when it is appropriate to use them.
		• Vehicle registration system is in place, but is not enforced. Not enforcing a policy that has been designed nullifies its need to exist.
		• No protocols or training for recognizing suspicious or illegally parked vehicles.

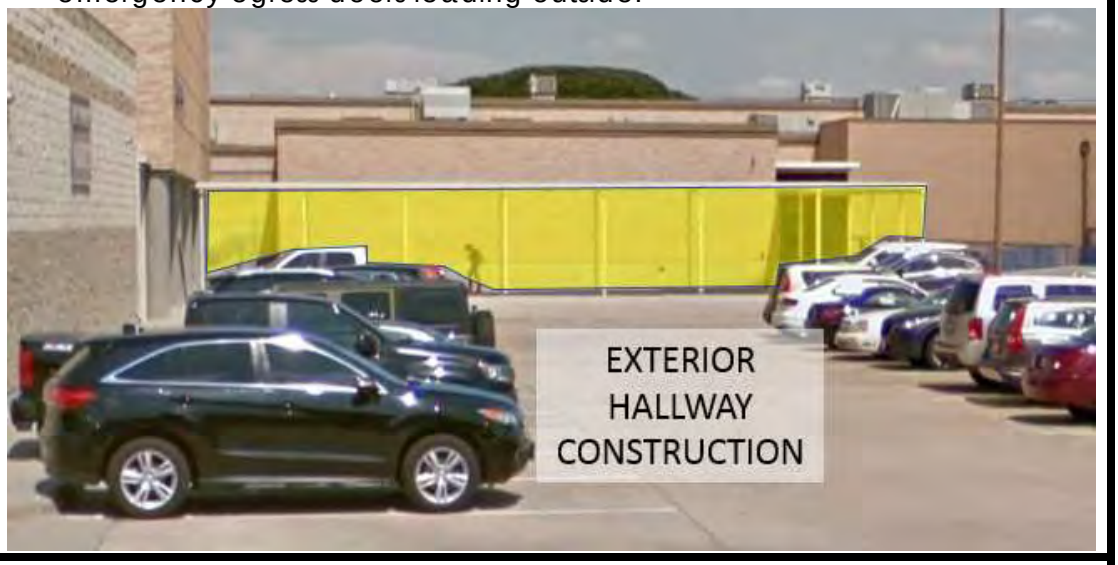
	Corrective Action	The following protective measures should be present at [redacted] High School to deter, detect, and prevent unauthorized access or malicious activity occurring at the perimeter: • Ensure that security cameras provide full coverage of the perimeter, parking areas, and vehicle access points. • Consider installing Automatic License Plate Recognition (ALPR) cameras, which may be used to identify vehicles that are stolen or belong to individuals with active criminal warrants.

- During arrival/dismissal, trained school staff should be responsible for monitoring security cameras that cover the vehicle entrances.
- Install lights utilizing high-efficiency LED bulbs to illuminate the entire property perimeter to a minimum horizontal illuminance of 10 lux. Vertical illuminance should be 25 percent of the horizontal illuminance or 2-3 lux. Ideally, exterior lamps should remain constantly illuminated throughout the night. To conserve energy, motion sensors may be installed on lights at areas where few pedestrians are expected late at night.
- Blue-light emergency call towers should be installed throughout the schools' parking areas. Though generally more expensive, blue-light help towers have a greater protective value compared to wall-mounted intercoms as their high visibility provides a level of deterrence against would-be perpetrators. The ideal standard is to have one emergency call tower every 40 feet.

		• Frequent perimeter and parking area checks should be conducted as part of recommended security coverage. Staff should enforce vehicle registration policy as to identify unauthorized vehicles and determine what their reasoning is for being on school property.
2	Threats and Vulnerabilities	<u>Exterior Property Access Control</u> The following access control deficiencies allow for a criminal to gain access to [redacted] High School's property: • Property is not entirely surrounded by perimeter fencing. This deters climbing, and if the fence is strong enough, prevents intentional or accidental vehicle ramming situation. • The vehicle gates are always open. This allows unauthorized vehicles to access the school.
	Corrective Action	• Properties should be completely enclosed by a perimeter fence. The fence should be of sufficient height and quality so it cannot be easily circumvented. • Install emergency egress gates to provide students and staff with security inside the building. Gates should be placed outside all exterior doors and implemented among recommended fencing. • Implement the following measures to better control access at vehicle entry points: o Vehicle entrances should have surveillance coverage and should be monitored during all arrival and dismissal periods by a staff member who is responsible for verifying, via video intercom, that all vehicles

		attempting to gain access have a legitimate purpose for being inside the property. o Securable vehicle gates should be present at all entry points and should be locked during periods outside of normal arrival and dismissal. The school should designate a single vehicle access point at which a mechanical barrier gate will be present. The barrier gate should be equipped with a card reader to enable access for school staff, and a video intercom to enable access for vendors and visitors.
3	Threats and Vulnerabilities	<u>Building Exterior</u> • Concealment areas along the building such as trees and low-level vegetation provide a hidden area for a criminal to plant explosive devices, biochemical devices or other malicious items. • Adjacent to the student entrance, the building is structured in an indented fashion that is not adequately monitored and a malicious item could be planted along the wall.

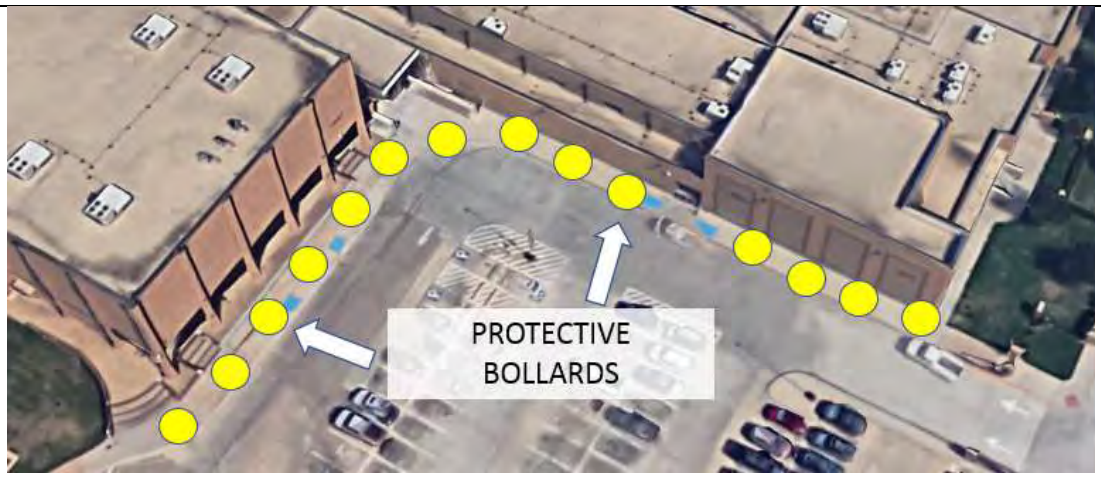
		• Garbage cans around the building are blue and of opaque material. This prevents security personnel from recognizing harmful items that may have been placed inside. • Classroom numbers are not posted on exterior windows. This information, when shared with first responders and law enforcement, enable these teams to quickly locate where a developing situation is occurring. • Consultants noticed all sets of double doors along the building's exterior have been configured in a way that they can be chained shut. This was the tactic used in the Virginia Tech shooting to prevent students and staff from escaping. In addition, this can delay first responder response times.  • There are three buildings that remain unlocked during all hours that school is in session: Junior ROTC, METSA, and F-Hall. The door linking the overhanging shelter from the main building to METSA is also left unlocked and unmonitored. In addition, the door linking the overhanging shelter from the main building to F-Hall is left unlocked and unmonitored. • The exterior door into Main Electrical Service room was left unlocked and consultants gained access to multiple critical utilities. The room also has unprotected exterior windows that could be intentionally shattered.
	Corrective Action	The following strategies help the school deter and prevent a criminal from harming students or the building: • Eliminate low-level bushes next to the building's exterior. If the school would prefer a more aesthetic looking exterior, they may opt to use taller bushes with nude bases which will provide easier inspection of the ground. • It is recommended that trash cans on the property are transparent to provide security staffing with easier detection of malicious items which may have been planted inside. • Add cameras to concealment area next to student's entrance. • Add classroom numbers to all exterior windows, and share new maps with law enforcement, first responders, and district administrators. • Install crash bar door handles that cannot be chained shut.

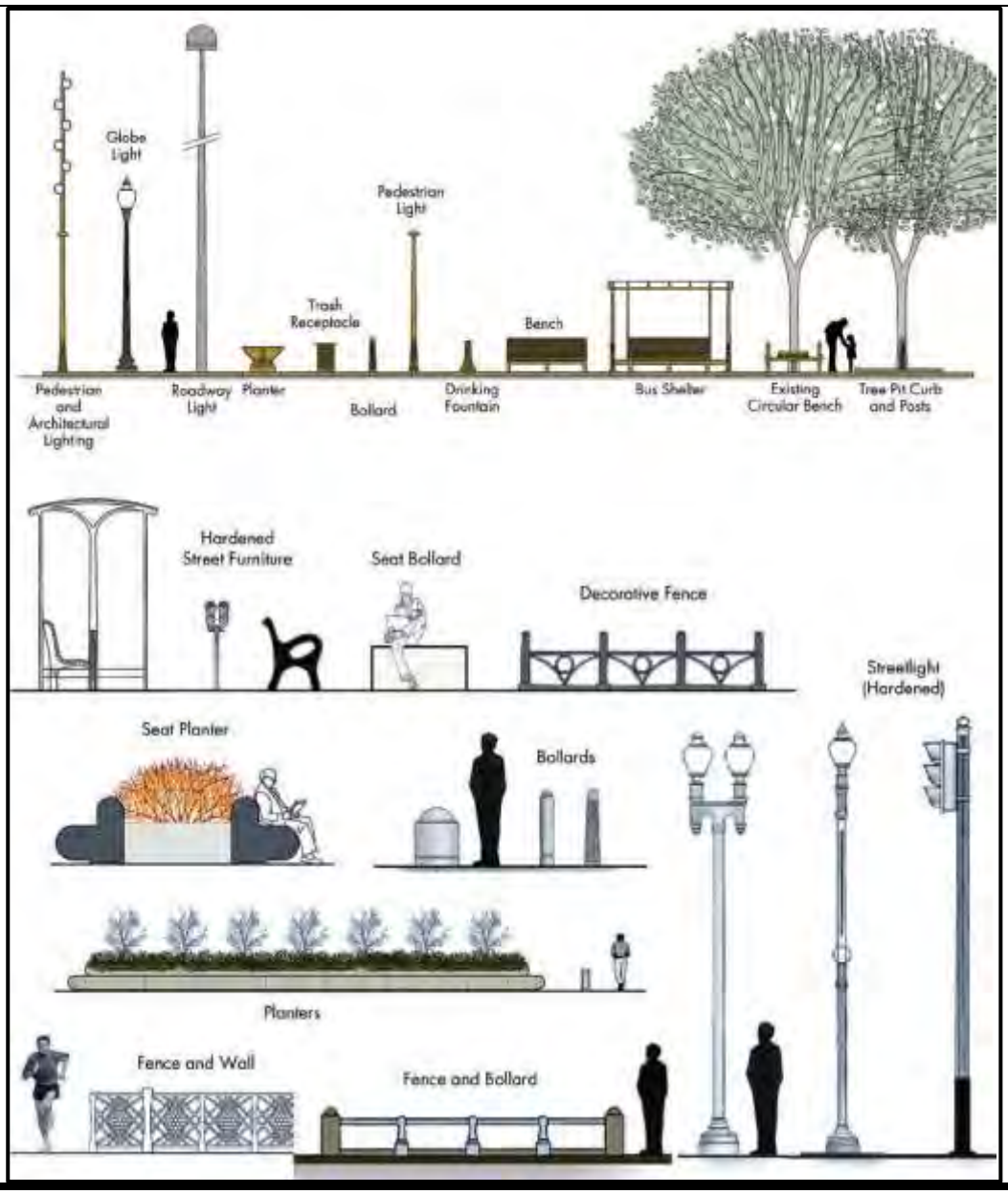
		• Doors designated solely for emergency egress should have their exterior handles removed. Furthermore, they should emit an audible alarm as well as transmit a signal to the main office that it has been opened. • The two main building entrances with the overhanging shelter attachments should be locked and should grant access via card reader. During passing periods, teachers should be designated to monitor these areas when students go outside to enter the F-Hall or METSA buildings. • Ideally, the two overhanging shelters referenced above should be constructed into hallways so students do not have to go outside. In addition, there should be an exterior hallway constructed between METSA and Junior ROTC buildings. These hallways should be installed with emergency egress doors leading outside. 
4	Threats and Vulnerabilities	<u>Critical Utilities – Exterior</u> Consultants noted during property walk-throughs that many exterior ground-level utilities, including electrical, natural gas, and relevant HVAC infrastructure, are exposed to malicious pedestrian and vehicle access. Furthermore, these areas are not adequately covered by security cameras, nor are they regularly checked for security threats by school staff. Loss of any of these utilities would have varying impacts on school operations, up to and including cancellation of all school activities.

	Corrective Action	The following measures should be present to protect exterior ground-level utilities against malicious attacks: • A secure enclosure should be constructed around all exposed electrical, natural gas, water, and HVAC infrastructure. The enclosure should be clear of vegetation and concealment areas and should not be used to store other equipment. • When located in areas experiencing frequent vehicle traffic, infrastructure should be protected by bollards or other vehicle crash barriers. • Utilities should be directly covered by security cameras and should be regularly checked for security threats by designated school staff.
5	Threats and Vulnerabilities	<u>Garbage Dumpsters</u> Consultants noted that garbage dumpsters at all locations were unsecure and easily accessible. Unsecured dumpsters may attract homeless individuals or criminals as they can be used to hide harmful or illicit materials, or as a potential source of supplies.

	Corrective Action	Areas containing garbage dumpsters should be stored inside a secured enclosure and must remain locked at all times. They should be clear of vegetation and concealment areas and should not be used to store other equipment. These areas should also be regularly monitored via security cameras and patrols.
6	Threats and Vulnerabilities	<u>Athletic Fields</u> The following deficiencies at the baseball field and track leave students and staff susceptible to crimes such as assault and kidnapping: • Lighting automatically turns off at midnight preventing students and staff from feeling secure as they move from school property to school property. • No camera coverage at either location. • There are no emergency call boxes at either location. This provides the opportunity for immediate contact to law enforcement if someone is on the fields late at night, authorized or not. • Emergency PA system does not reach either location. This is dangerous as it does not alert individuals in the areas of a potential emergency occurring at the main school building.
	Corrective Action	The steps below can help reduce the chance of an emergency at the baseball field and track: • Install motion-sensored lighting to save energy but also provide individuals with level of safety while they are at the athletic areas. Lights should shine at a minimum of 10 lux. • Expand camera coverage and ensure these areas are monitored. • Install emergency call boxes on perimeter of both fields.

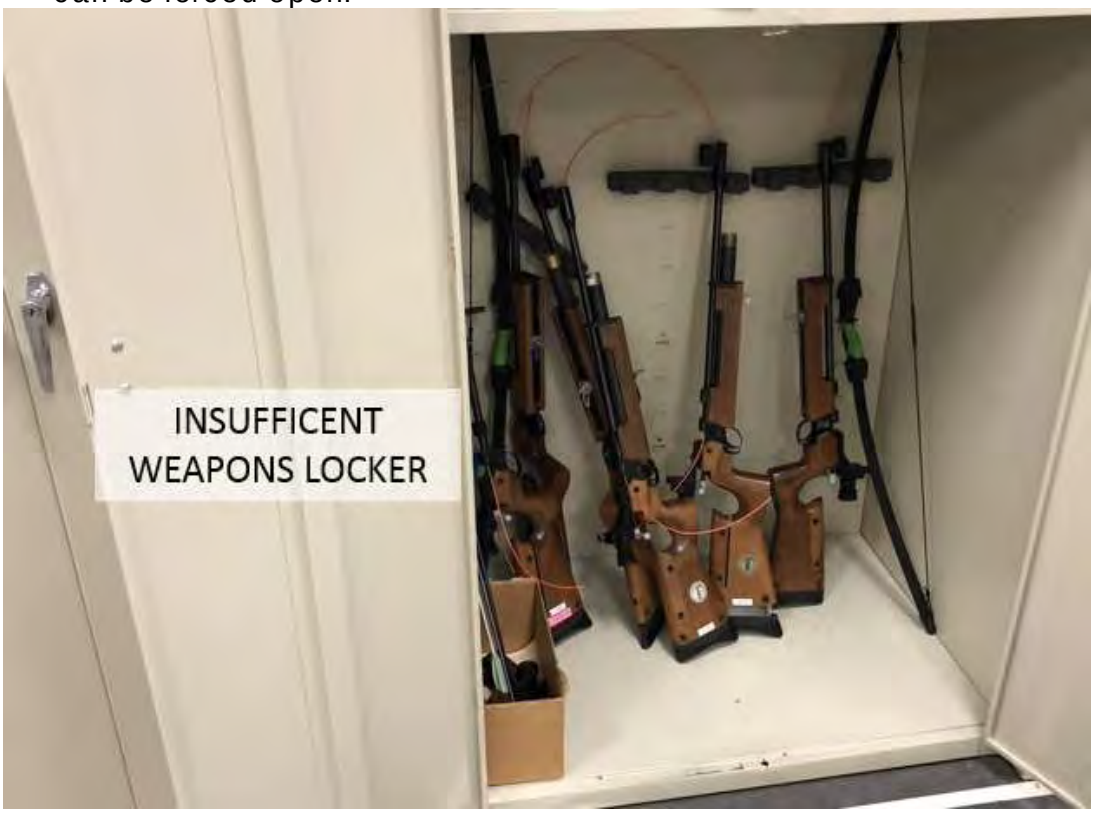
		 • Add PA intercom speakers to both fields and ensure those on the track can clearly hear messages being relayed from the main campus.
7	Threats and Vulnerabilities	<u>Vehicle Standoff Protection</u> With the exception of bollards near exterior utilities on the West side of the school, vehicle standoff protection is not present at [redacted] High School. This greatly increases the exposure of students and staff to accidental or intentional vehicle ramming, especially along primary walkways and near primary building access points. At the Southeast entrance, the main building entryway for students, there are no protective measures in place and a criminal would be able to drive up and intentionally vehicle ram during arrival or dismissal.
	Corrective Action	Ideally, standoff measures should be installed at all pedestrian walkways and building entrances that are exposed to vehicle traffic. Minimally, standoff features should be present at primary walkways and building entrances. Standoff features should adhere to the following functional requirements: • Barriers should have a minimum Department of State crash rating of K4, which will prevent a 15,000-lb. Vehicle traveling at 30 miles-per-hour from penetrating more than 36 inches past the barrier. • Bollard spacing should be between 36 and 48 inches (0.9 and 1.2 meters) depending on the kind of traffic expected and the needs of pedestrians and the disabled.

		 • When a long line of bollards is unavoidable, the bollards are to be interspersed with trees and oversized bollards that can act as seats. In a few years, the trees will dominate the streetscape, and the barriers will be unobtrusive. • Bollards should be kept clear of ADA access ramps at the corner quadrants at streets. • In place of bollards, the school may choose to install protective planters, benches, and permanent concrete sculptures to maintain the aesthetics of the school.

		
8	Threats and Vulnerabilities	<u>Main Entrances</u> Main entrances are the primary locations for enforcing access control and ensuring that only approved individuals with a legitimate purpose are able to enter and remain inside the building. The following physical and procedural deficiencies create the potential for pedestrian tailgating, forced entry, or access into the school under false pretenses: • Main doors are unlocked during hours of operation. • Lack of video intercom prohibits main office from screening individuals before they enter the school. • Main office receptionist does not have clear view of the main hallway. As a result, they are unaware of individuals making their way inside, thus eliminating any vetting they need to accomplish.

	Corrective Action	The following measures should be present at the main entrance to improve access control capabilities: • Physical modifications are recommended at main entrances and lobbies to ensure that visitors and vendors/contractors are physically obliged to stop inside the main office before continuing through the rest of the building. • Secretary's desk should be moved close to the hallway and the partition between them and outside the office should be a teller window. A secure portal should be constructed that provides communication but also keeps the administrative staff from malicious individuals. Window should also have a slot installed to provide exchanging of documents between parties. • Video intercom should be put outside the main visitor's entrance to enable main office to speak and view those attempting to enter. • Ideally, both sets of doors in the main entrance should be moved West several feet and the vestibule wall installed in their place. This keeps the main office safe as it requires the individual to be screened, buzzed in by secretary, and then they may enter the office or other parts of the school. • School staff and volunteers should be reminded of prohibitions against pedestrian tailgating as well as proper steps to be taken if an unidentified individual attempts to follow a staff member into the school.
9	Threats and Vulnerabilities	<u>Layout & Design</u> • The current school layout encompassing eight buildings with no access controls between them is one of the larger vulnerabilities of the property. Students are required to go to outside to get to certain classes, and the doors used to enter these buildings are universally unsecured. • Doors leading to the courtyard are left unlocked which provides easy access to and from the roof into the school for a criminal. • Doors leading to the attic above the automotive garage are left open and that provides access to the roof where a criminal has a myriad of attacks that can be carried out. These include poisoning the HVAC units, using the roof as strategic position while actively shooting individuals, tampering of critical utilities, and others.
	Corrective Action	• Through mobile apps, students can access buildings secured with radio-frequency identification (RFID) readers with Bluetooth capabilities via their smartphones. These doors should be on a schedule and should be allowed to open when students are authorized to be on the property. Thorough auditing of each door should be done to determine if RFID readers are necessary. • Courtyard doors should be access controlled, and if students and staff need to escape during a fire, there can be a delayed egress to provide access to courtyard. • Attic doors should be locked at all times and installed with an alarm. Dual-factor authentication is recommended as well, such as a PIN pad and access card. Camera coverage is recommended as well.

10	Threats and Vulnerabilities	<u>Hallways & Lockers</u> • Consultants noted that the school has no way to segment the buildings into secure sections during emergency scenarios. This can increase the potential exposure of students and staff during an armed intruder scenario, as the aggressor will be able to move freely through the building. • Lockers are never checked for drugs or malicious items students may be storing.
	Corrective Action	• Emergency segmentation doors should be incorporated into the hallways of the school and should be integrated into automatic lockdown capability. In the event of an armed intruder scenario, this feature would limit the ability of the intruder to move through the building. • Part of security protocols should be to do random and non-random checks of lockers. This will deter students from harboring malicious items if they know the security teams are doing locker checks.
11	Threats and Vulnerabilities	<u>Classrooms and Office Spaces</u> The following deficiencies may decrease the ability of students and staff to effectively shelter during an armed intruder scenario: • Impact protection is not present on interior doors, windows, and sidelights at offices and classrooms. Additionally, most of these spaces do not have interior blinds to obscure an aggressor's view from the hallway. • Consultants noted that in most cases, interior locking capability is not present on classroom and office doors. During an incident requiring a

		lockdown, occupants may be unable to easily secure these rooms without first stepping out into the hallway, thereby exposing themselves to the danger. The ability to quickly lock down classrooms is further complicated by the common practice of keeping the classroom key inside the storage room. • Weapons (non-lethal) in the Junior ROTC are easily accessible because the building is left unlocked and the weapons are kept in cabinets that can be forced open.  • Nursing classroom utilizes one level of security. This is not enough to prevent students or staff from stealing highly expensive equipment from this area.

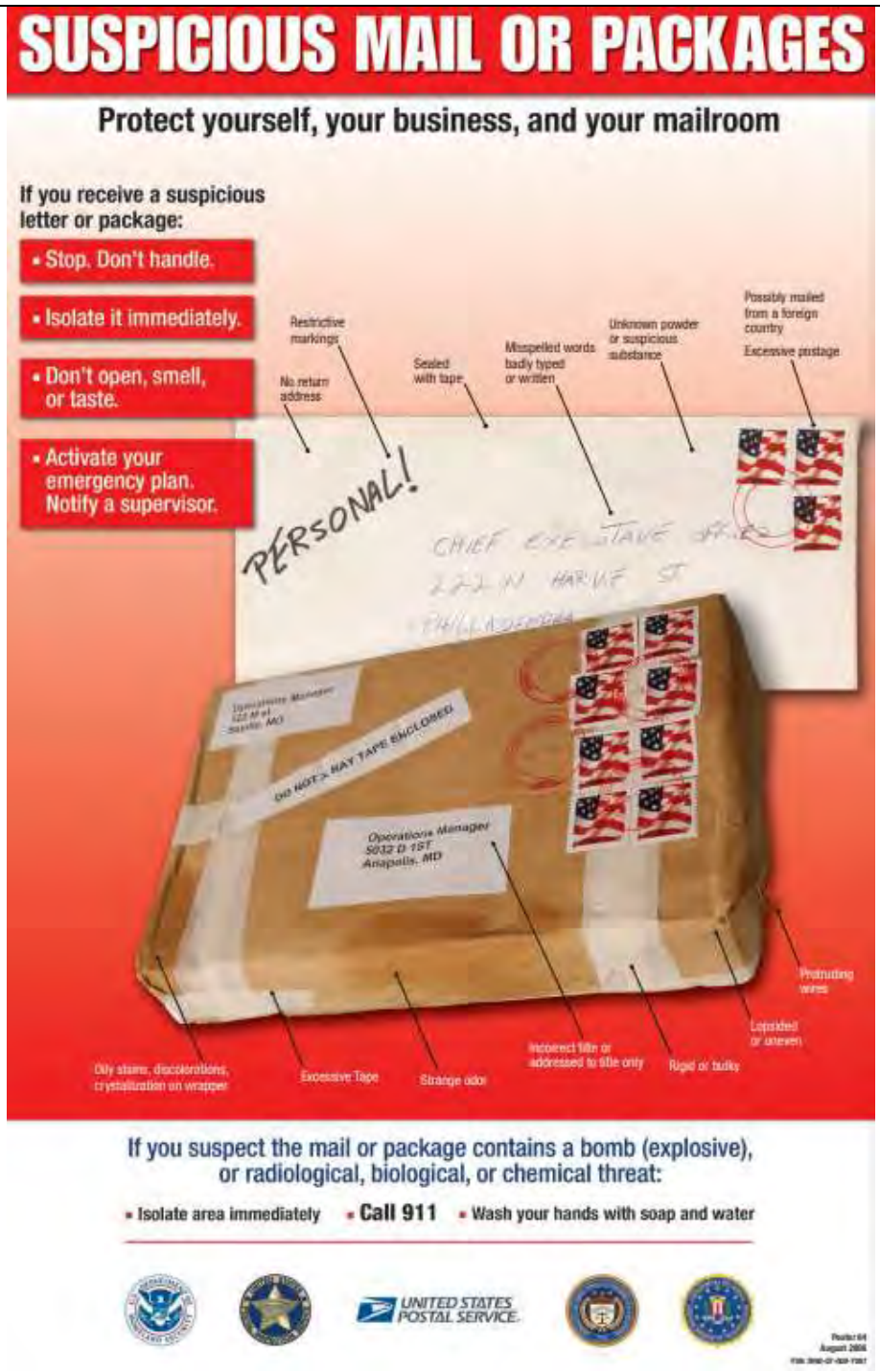
	Corrective Action	The following measures should be implemented to improve the protection of students and staff during armed intruder scenarios: • Interior doors at all classrooms and offices should have the capability of being locked from the inside without requiring an individual to step out into the hallway. Ideally, interior door handles should have thumb locks or similar mechanisms. Alternatively, doors may remain permanently locked with a magnet or easily removable device attached to the door so that the door will not completely close unless necessary. • Ensure that doors at designated classroom shelter spaces (storage rooms and bathrooms) are constructed from solid wood or metal, do not contain windows, and can be locked from the inside. • Weapons should be kept in proper weapon lockers. Access to lockers should have two-factor authentication and Junior ROTC doors should be locked and windows should be hardened or laminated. • Nursing classroom should implement a second layer of security to prevent theft and sabotage to valuable items. Window on door should be removed or laminated/hardened.
12	Threats and Vulnerabilities	<u>Administrative and Critical Utility Spaces</u> • Students' filing cabinets are left unlocked during the day and are usually left that way overnight when the offices are vacant. This provides malicious individuals with the opportunity for theft or vandalism of vital students' documents.

		 • Medicine in the nurse's office is only secured via one layer of access control. Office is usually left unlocked and it is feasible that an unstable individual could tear the medicine door off the hinge.

		 • Main Distribution Frame (MDF) room is left unlocked and can be sabotaged and vandalized by anyone with malintent. This would disrupt school operations for an extended period. • A/V storage room inside the library is unlocked and left open. Items inside may be stolen or sabotaged.
	Corrective Action	• Ensure all student filing cabinets are always locked unless authorized individuals are using contents within. At the end of the day, main office staff should be responsible for locking the cabinets. • Nurse's office should be equipped with card-reader access to ensure only individuals escorted by the nurse are allowed inside. The only time it should be left unlocked is when the nurse is physically inside the office. • MDF and A/V rooms must have at a minimum card-reader access control with intrusion sensors that alert the main office if unauthorized access has been committed. Furthermore, the exterior and interior of both rooms should be under security camera coverage.
13	Threats and Vulnerabilities	<u>Culture of Security</u> Staff does not play an active role in maintaining the security of their place of work. As a result, there is an increased likelihood that violent and non-violent

		threats that are still in the pre-operational phase will either go unnoticed or unreported. Contributing deficiencies include the following: • School does not have any form of an ongoing, mandatory security education and awareness program. • No initiation of any campaigns to make security related information easily visible and accessible throughout regularly occupied areas.
	Corrective Action	An essential pillar of a successful security program is the organization's culture of security and the overall security awareness of all non-security occupants. [redacted] should implement an ongoing security awareness program targeted at all staff and occupants. This program should provide a combination of periodic mandatory security awareness training and continuous informational campaigns to ensure that security remains at the forefront of occupants' minds. • Mandatory security awareness training for non-security occupants should minimally occur on an annual basis and should address the following topic: o Common indicators of potentially threatening individuals, items, and vehicles, including techniques for detecting these indicators. o Order of procedures to be followed once an individual has detected a potential threat indicator. • The school should ensure that regular drills and exercises address security-related scenarios such as attempted intrusion, suspicious behavior, or potential-IED.
14	Threats and Vulnerabilities	<u>Receiving Areas and Protocol</u> • There is no formalized effective protocol for verifying delivery items and personnel. This increases the potential for an unauthorized individual or item to enter the school if a new school staff member is working at the receiving area, or if receiving staff choose to simply trust a previously unknown delivery person. • Sysco has access to the school at night to load and unload goods. Like above, this grants a criminal unlimited access to the school where they can plant explosive or biochemical devices to detonate when the school is busy.
	Corrective Action	• Additional exterior security cameras should be installed to provide full coverage of the buildings' receiving areas. Cameras should also provide coverage of the receiving area interiors. • [redacted] High should have a well-defined policy that addresses the practice of receiving deliveries at the north receiving area. It should include the following components: o Vendor companies should provide schools with a list of approved drivers and vehicles. Required information should include drivers' names, license numbers, and company ID numbers (if available), as well as vehicle makes, models, and license plate numbers. Receiving staff should verify drivers and vehicles upon arrival. o School receiving staff should have a list of expected contents for specific delivery vehicles. That list should be compared to the work order provided by the driver at the time of arrival.

		• Disallow Sysco from having access to the school. Instead, the district's monitoring center should be responsible for screening the Sysco employee and buzz them in only when they are positive of the individual's identity.
15	Threats and Vulnerabilities	<u>Mail Protocol</u> • Incoming mail is not screened for threat indicators before it is distributed to final recipients. This deficiency means potentially exposing school staff to mail-borne threats. • Like above, there is no staff trained in detecting what qualifies as a suspicious package. Items are blindly sent to their destination without any suspicion that it could be harmful. • If an item is believed to be harmful, there are no protocols in place on how to determine if the suspicion is true.
	Corrective Action	All incoming mail and packages should be screened for threat indicators by specially trained staff before items are distributed to their final recipients. Employees who are expected to handle and process incoming mail should be trained to detect and address potential threat indicators.

		
16	Threats and Vulnerabilities	<u>Cafeteria & Kitchen</u> • During school hours, refrigerators in the kitchen are not under surveillance and are left unlocked. This leaves food and beverage items open to sabotage and potential poisoning of students and staff.

		 • There are no security staff dedicated to being present during lunch hours and therefore, there are no sweeps of the lunch room prior to lunch periods to check for malicious items.
	Corrective Action	• Refrigerators should always be locked and kitchen staff members given a PIN code that provides access. • Part of the security staffing protocols will be to have stationed lunch room personnel to ensure students are entering a safe area every day.

Vulnerability Analysis

The following assessment evaluates vulnerabilities that can be exploited by an aggressor to damage critical assets across a broad range of identified PMAs. It provides a basis for determining mitigation measures for the protection of each facility's critical assets.

The vulnerability analysis is based on the review of existing deficiencies within the current security program, and how these deficiencies affect the exposure of occupants and other high-value assets to relevant threats. It is important to note that the vulnerability analysis table does not consider the relative value of each asset. Furthermore, it assumes that the likelihood that each threat will be attempted is 100 percent.

Vulnerability Rating	
Very High	10
High	8-9
Medium-High	7
Medium	5-6
Medium Low	4
Low	2-3
Very Low	1

Vulnerability Rating Table

Very High – One or more major weaknesses have been identified that make assets extremely susceptible to an aggressor or hazard.

High – One or more significant weaknesses have been identified that make assets highly susceptible to an aggressor or hazard.

Medium High – An important weakness has been identified that makes assets very susceptible to an aggressor or hazard.

Medium – A weakness has been identified that makes assets fairly susceptible to an aggressor or hazard.

Medium Low – A weakness has been identified that makes assets somewhat susceptible to an aggressor or hazard.

Low – A minor weakness has been identified that slightly increases the susceptibility of assets to an aggressor or hazard.

Very Low – No weaknesses exist.

Vulnerability Analysis Table

	ASSETS									
	People	Building	Utilities	Specialty Equipment for Specialized Programs	Data and Telecom Infrastructure	Chromebooks	Student/ Personnel Files	Medication	Outside Facilities (Athletic)	Cash/ Checks
PMA	Vulnerability Rating	Vulnerability Rating	Vulnerability Rating	Vulnerability Rating	Vulnerability Rating	Vulnerability Rating	Vulnerability Rating	Vulnerability Rating	Vulnerability Rating	Vulnerability Rating
Shooting	9	1	1	1	1	1	1	1	1	1
Assault	7	1	1	1	1	1	1	1	1	1
Vandalism	1	5	6	7	4	4	5	2	7	1
Vehicle Ramming	10	8	7	1	1	1	1	1	1	1
Theft	1	1	1	4	6	4	6	3	1	3
Burglary	1	5	1	7	6	4	6	2	1	1
Arson	2	5	7	3	6	2	6	2	1	2
Improvised Explosive Device	9	9	9	5	6	1	1	1	6	1
Sabotage	4	7	7	5	6	2	1	3	4	2
Car Bomb	9	9	9	1	1	1	1	1	6	1
Chemical/Biological Weapon	6	1	1	1	1	1	1	1	1	1
Mail/Package Device	6	5	1	1	1	1	1	1	1	1

Risk Assessment Analysis

The purpose of this risk assessment analysis is to provide the decision makers of the school with a foundation for a risk management plan.

Risk is the potential for a loss of or damage to an asset. It is measured based upon the value of the asset and consequences of an attack in relation to the threats and vulnerabilities associated with it. Risk is based on the likelihood or probability of a PMA occurring, and the consequences of the occurrence. This risk assessment analyzes the threat (probability of occurrence), asset value (consequences of the occurrence), and vulnerabilities to ascertain the level of risk for each asset against each applicable PMA. Thus, a very high likelihood of occurrence with very small consequences may require simple, low-cost mitigation measures, but a very low likelihood of occurrence with very grave consequences may require costlier and complex mitigation measures.

Risk Number (Per Asset)	Risk Rating
≥ 261	Very High
201-260	High
141-200	Medium High
101-140	Medium
61-100	Medium Low
31-60	Low
1-30	Very Low

Risk Assessment Rating Table

Very High – The potential for loss of or damage to the critical assets is so great as to expect exceptionally grave consequences such as extensive loss of life, widespread severe injuries, or total loss of primary services and core functions and processes.
High – The potential for loss of or damage to the critical assets is so great as to expect grave consequences such as loss of life, severe injuries, loss of primary services, or major loss of core functions and processes for an extended period of time.
Medium High – The potential for loss of or damage to the critical assets is such as to expect serious consequences such as serious injuries, or impairment of core functions and processes for an extended period of time.
Medium – The potential for loss of or damage to the critical assets is such as to expect serious consequences such as injuries or impairment of core functions and processes.
Medium Low – The potential for loss of or damage to the critical assets is such as to expect only moderate consequences such as minor injuries, or minor impairment of core functions and processes.
Low – The potential for loss of or damage to the critical assets is such as to expect only minor consequences or impact such as a slight impact on core functions and processes for a short period of time.
Very Low – The potential for loss of or damage to the critical assets is so low that there would be only negligible consequences or impact.

Risk Analysis Table

PMAs	People	Building	Utilities	Specialty Equipment for Specialized Programs	Data and Telecom Infrastructure	Chromebooks	Student/ Personnel Files	Medication	Outside Facilities (Athletic)	Cash/ Checks
Shooting	**900**	**90**	**70**	**50**	**90**	**10**	**50**	**80**	**10**	**10**
Asset Value	10	9	7	5	9	1	5	8	1	1
Threat Rating	10	10	10	10	10	10	10	10	10	10
Vulnerability	9	1	1	1	1	1	1	1	1	1
Assault	**560**	**72**	**56**	**40**	**72**	**8**	**40**	**64**	**8**	**8**
Asset Value	10	9	7	5	9	1	5	8	1	1
Threat Rating	8	8	8	8	8	8	8	8	8	8
Vulnerability	7	1	1	1	1	1	1	1	1	1
Vandalism	**70**	**315**	**294**	**245**	**252**	**28**	**175**	**112**	**49**	**7**
Asset Value	10	9	7	5	9	1	5	8	1	1
Threat Rating	7	7	7	7	7	7	7	7	7	7
Vulnerability	1	5	6	7	4	4	5	2	7	1
Vehicle Ramming	**600**	**432**	**294**	**30**	**54**	**6**	**30**	**48**	**6**	**6**
Asset Value	10	9	7	5	9	1	5	8	1	1
Threat Rating	6	6	6	6	6	6	6	6	6	6
Vulnerability	10	8	7	1	1	1	1	1	1	1
Theft	**70**	**63**	**49**	**140**	**378**	**28**	**210**	**168**	**7**	**21**
Asset Value	10	9	7	5	9	1	5	8	1	1
Threat Rating	7	7	7	7	7	7	7	7	7	7
Vulnerability	1	1	1	4	6	4	6	3	1	3
Burglary	**50**	**225**	**35**	**175**	**270**	**20**	**150**	**80**	**5**	**5**
Asset Value	10	9	7	5	9	1	5	8	1	1
Threat Rating	5	5	5	5	5	5	5	5	5	5
Vulnerability	1	5	1	7	6	4	6	2	1	1

PMAs	People	Building	Utilities	Specialty Equipment for Specialized Programs	Data and Telecom Infrastructure	Chromebooks	Student/ Personnel Files	Medication	Outside Facilities (Athletic)	Cash/ Checks
Arson	100	225	245	75	270	10	150	80	5	10
Asset Value	10	9	7	5	9	1	5	8	1	1
Threat Rating	5	5	5	5	5	5	5	5	5	5
Vulnerability	2	5	7	3	6	2	6	2	1	2
Improvised Explosive Device	540	486	378	150	324	6	30	48	36	6
Asset Value	10	9	7	5	9	1	5	8	1	1
Threat Rating	6	6	6	6	6	6	6	6	6	6
Vulnerability	9	9	9	5	6	1	1	1	6	1
Sabotage	200	315	245	125	270	10	25	120	20	10
Asset Value	10	9	7	5	9	1	5	8	1	1
Threat Rating	5	5	5	5	5	5	5	5	5	5
Vulnerability	4	7	7	5	6	2	1	3	4	2
Car Bomb	360	324	252	20	36	4	20	32	24	4
Asset Value	10	9	7	5	9	1	5	8	1	1
Threat Rating	4	4	4	4	4	4	4	4	4	4
Vulnerability	9	9	9	1	1	1	1	1	6	1
Chemical/Biological Weapon	180	27	21	15	27	3	15	24	3	3
Asset Value	10	9	7	5	9	1	5	8	1	1
Threat Rating	3	3	3	3	3	3	3	3	3	3
Vulnerability	6	1	1	1	1	1	1	1	1	1
Mail/Package Device	120	90	14	10	18	2	10	16	2	2
Asset Value	10	9	7	5	9	1	5	8	1	1
Threat Rating	2	2	2	2	2	2	2	2	2	2
Vulnerability	6	5	1	1	1	1	1	1	1	1
Total Asset Risk	3750	2664	1953	1075	2061	135	905	872	175	92
Total Organization Risk	13682									

Protective Measures Summary and Prioritization

A successful security system encompasses security measures that can deter, prevent, detect, and respond to perpetrators' PMAs. TNCG understands that budget limitation will not allow for the implementation of all security measures at once. Therefore, it is important to have a prioritization guideline to allow for the implementation of most urgent, cost-effective, and multi-purpose protective measures.

The following tables outline the method and rationale behind the prioritization of each recommended protective measure at the school.

Criteria	Description	Protective Value
Deter	The protective measure is capable of deterring potential perpetrators from executing the PMA.	Greatest protective value.
Prevent	The protective measure is capable of preventing the specific PMA being carried out against the facility and its assets.	High protective value.
Detect	The protective measure will allow the facility to detect a perpetrator before an incident occurs.	Medium protective value.
Respond	The protective measure will enhance the response of the security unit, emergency response team, and law enforcement agencies.	Lowest protective value.
Multi-Purpose	The recommended protective measure is capable of performing two or more functions.	Combined protective value incorporating at least two of the following: deterrence, prevention, detection, or response capabilities.

Protective Measures Assessment Table

In order to rank and classify the criticality and priority for implementation of security measures, the following guideline is used.

Priority Ranking	Ranking Description
Very High Priority	Recommended protective measures are critical for the mitigation of the most critical, very high-risk PMAs at this site. These protective measures require immediate implementation.
High Priority	The recommended protective measures are significant for the mitigation of high-risk PMAs at this site. These protective measures should be initiated within the coming one to two years.
Medium Priority	The recommended protective measures will play an important role in the mitigation of medium to medium-high risk PMAs at this site. These protective measures should be incorporated into a multi-year budget plan.
Low Priority	The recommended protective measures will play a secondary role in supporting the first-, second-, and third-priority protective measures in the mitigation of low-risk PMAs at this site. These protective measures should be incorporated into a multi-year budget plan.

Protective Measures Ranking Table

Protective Measures Prioritization Guideline

In addition to the Ranking Value Assessment, this guideline considers the Risk Assessment score as it relates to the organization's operational environment to ensure that recommended measures are ranked based on their ability to reduce the total risk.

Priority	Protective Measure	Findings and Recommendations Item Number:
Very High	Exterior Detection: Camera coverage of perimeter, staff monitoring vehicle entrance cameras, perimeter illumination, blue-light call towers, ALPR, perimeter security checks.	1
Very High	Main Entrance: Secure vestibule, video intercom outside main entrance, move secretary's desk, prohibitions against tailgating.	2
Very High	Classrooms: Impact protection/blinds, shelter space doors upgrade, ROTC weapons closet improvement, dual-factor security for nursing classroom.	11
Very High	Culture: Mandatory awareness training, regular drills and exercises for staff and students.	13
Very High	Layout & Design: RFID access to building entrances.	9
High	Building Exterior: Eliminate concealment areas, transparent trash cans, crash bars on exterior doors, classroom numbers posted on exterior windows, turn overhanging shelters into hallways, RFID capabilities to access other buildings, outer handles removed from egress doors.	3
High	Exterior Utilities: Secure enclosure around all infrastructure, bollards around utilities near high vehicle traffic areas, surveillance coverage of utilities.	4
High	Vehicle Standoff Protection: Bollards/benches/planters near high student-traffic walkways.	7
High	Exterior Perimeter Access Control: Property enclosed by fencing, CCTV coverage and card readers at vehicle	8

	entrances, egress gates in perimeter fencing.	
Medium	Layout & Design: Courtyard doors access-controlled, dual-factor authentication for attic doors.	9
Medium	Hallways: Emergency segmentation capabilities, random/non-random locker checks.	10
Medium	Receiving Area: Security cameras added, delivery system software, disallow Sysco from having school access.	14
Medium	Mail Protocol: Train staff to recognize potentially threatening packages.	15
Low	Dumpsters: Build secured enclosure, install security camera coverage.	5
Low	Athletic Fields: Motion-sensor lighting, add camera coverage, call boxes around areas, add PA intercom.	6
Low	Administrative & Critical Utility Spaces: Filing cabinets always locked, card-reader access for nurse's office, minimum of card-reader access and camera coverage to MDF and A/V rooms.	12
Low	Cafeteria: PIN pad on refrigerators, designated lunch room security personnel.	16

Conclusion

As part of its assessment of the school, TNCG developed the organization's target profile, which identifies the most likely PTEs that may target the school and assets. These include both violent and non-violent actors driven by idiosyncratic, criminal, and ideological motives. Relevant PTEs may employ various PMAs such as shooting, assault, vandalism, theft, burglary, arson, or vehicle ramming to harm the organization and its assets.

The observations described above focus on the major aspects of the school's security program and threat profile. The primary purpose of this report is to improve the school's ability to proactively deter, detect, and ultimately prevent any potential malicious acts against the organization, and if necessary, respond in an effective manner that will minimize the potential consequences of any such act.

TNCG appreciates the opportunity to work with school personnel on this critical task of enhancing the safety and security of the school and school community.

Appendix I: CRIMECAST® Report

The CRIMECAST® report scores the predictability of crime-related threats at the national, state, and county levels. CRIMECAST® scores range between 0 and 2000, and a score of 100 represents the average level. A score above 100 means that this location is proportionately more likely to be subject to crime as it relates to a specific level. Below is a more detailed analysis of this specific location, highlighting significant trends and data points relating to the threat profile of the site.

SITE NAME: [redacted] High School		Past (2010)	Current (2018)	Projected (2023)
National	CAP Index	200	155	152
	Crimes Against Persons	133	87	84
	Crimes Against Property	83	62	55
State	CAP Index	192	149	140
	Crimes Against Persons	117	76	71
	Crimes Against Property	49	36	31

Based on the scores of the CRIMECAST® report, [redacted] is 1.55 times as likely to experience a crime as the average addressable location throughout in the United States, and 1.49 times as likely as the average addressable location in Texas.

CRIMECAST® Scoring Methodology

The CRIMECAST® scoring system is based on the strong relationship between a neighborhood's "social disorganization" and the amount of crime that occurs there. Social disorganization theory is closely linked to the "ecological perspective" of crime, delinquency, and human behavior, which views criminal activity as the product of weakly-organized social environments. This crime affects not only the immediate neighborhood, it also spills over to surrounding areas. The CRIMECAST® model considers potential travel patterns.

CRIMECAST® scores are generated by comparing criminal and loss-related reports against approximately 150 demographic predictors, including:[14]

- Population and age distributions.

[14] The analysis of neighborhood demographics excludes race, religion, and other protected categories.

- People living in group quarters (prisons, colleges, nursing homes, military installations, etc.).
- Housing values and trends.
- Family and household membership.
- Marital status.
- Home ownership vs. rentals.
- Nature of housing unit (attached, detached, multi-family, mobile home, etc.).
- Age of housing structure.
- Time lived in housing unit.
- Number of vehicles.
- Income amounts and sources (wages, investments, public assistance, retirement, etc.).
- Educational levels.
- Families/households below poverty level.
- Employment rates.
- Means of transportation to work (drive, car pool, public transportation, bike, walk, work from home, etc.).
- Travel time to work.

CAP Index is constantly testing its methodology by assessing neighborhood demographics against address-specific incidents. In 2017, Cap Index released a report in which it analyzed 7,888,341 address-specific crimes reported across the United States from 2014-2016. The results of the study have supported the CRIMECAST® scoring methodology.

For [redacted]'s CRIMECAST® report, Cap Index assessed two primary crime categories:

- Crimes Against Persons—This includes homicide, rape, robbery, and aggravated assault.
- Crimes Against Property—This includes burglary, larceny, and motor vehicle theft.

The overall CAP Index score expressed above takes into account all assessed crime types. Note: The overall CAP Index score does not equal the sum of the scores for crimes against people and crimes against property, as the CRIMECAST® model weights certain crime types more heavily than others when determining the location risk level.

Appendix II: Glossary of Common Terms

TNCG regularly refers to the following acronyms when discussing an organization's security program and relevant manmade intentional threats:

- AMO – Aggressor's Method of Operation. This refers to the various stages of a hostile plot targeting an organization, facility, or asset, from target selection and planning through execution.
- Assault – Intentional bodily harm inflicted by one or more assailants against one or more victims, with or without the use of blunt or edged weapons.
- Burglary – Unlawful entry into a building or facility to steal items or materials at a time when the building or facility would not otherwise be accessible to the public.
- IED – Improvised Explosive Device.
- IID – Improvised Incendiary Device.
- PMA – Potential Method of Action. A violent or non-violent action that an individual may take to cause injury, damage, or loss to an organization, facility, or asset.
- PTE – Potential Threat Element. An individual or group that may be motivated to target an organization, facility, or asset through violent or non-violent means.
- SRA – Security Risk Assessment. A combined analysis of a site's or organization's high-value assets, relevant threats, and existing vulnerabilities.
- Theft – Unlawful acquisition of items or materials during a period when the general area would be accessible to the public.
- VBIED – Vehicle-Borne Improvised Explosive Device.

Exhibit 15 – Options

Services Overview

DESCRIPTION OF SECURITY CONSULTING SERVICES PROVIDED BY TRUE NORTH CONSULTING GROUP	
Security Risk Assessments	Comprehensive, risk-based assessments of facilities and security programs utilizing DHS, FBI, and Israeli Shin Bet methodology. Assessments include risk analysis, threat assessment, vulnerability assessments, and mitigation recommendations. The goal of the assessment is to increase our client's ability to prevent, detect, deter, and respond to man-made threats to staff and visitors on facilities.
Threat Assessments	Comprehensive, community-specific threat assessments utilizing DHS and FBI methodology and incorporating up-to-date threat information from local and regional law enforcement, including regional FBI Fusion Center data and information.
CPTED Assessment and Mitigation	TNCG security and vulnerability assessments and mitigation recommendations include and address Crime Prevention Through Environmental Design (CPTED) principles.
Lighting Assessments	As part of our security assessments, TNCG will assess outside lighting levels for facilities and sites to ensure adequate levels of lighting for both prevention of threats as well as effective response to potential situations.
All-Hazards Mitigation	TNCG provides best practice all-hazard mitigation recommendations addressing based on security and vulnerability assessments. Mitigation recommendations are prioritized and address all three areas of security programs: physical, technology, and human factor security. Cost estimates are part of the mitigation recommendations if desired. Mitigation strategies are designed to address identified risks and threats.
Physical Security & Supporting Technology Infrastructure Design and Engineering, Acquisition & Project Management	True North provides these services in the following technologies: o Video Surveillance/CCTV o Identity Management o LAN (including Wireless LAN) o Access/Entry Control o Video Management Systems (VMS) o Video Analytics and Biometric Technologies o Alarm Systems/Intrusion Detection/Notification Systems o Communications/Dispatch Systems/Command Center
Security Master Planning	TNCG consultants provide security master planning services, providing our clients with a comprehensive, long-term strategy that covers all aspects of a security operation and provides sequential planning over a period of years to provide a safe, secure environment.

All-Hazards Emergency Management Planning	TNCG reviews emergency management plans, policies, and procedures, assists in updating plans and policies, and writes all-hazards emergency management plans for our clients. TNCG follows DHS and FEMA guidelines for emergency management planning, ensuring emergency management plans meet any local and state requirements.
Business Impact Analysis	TNCG assists clients in determining and evaluating the potential effects of an interruption to critical **business** operations as a result of a disaster, accident, or emergency, including IT functions.
Business Continuity Planning	With knowledge of the threats and risks faced by our clients, TNCG consultants work with them to create strategies and a plan to ensure that personnel and assets are protected and able to function in the event of an emergency both in the short-term and long-term.
Continuity of Operations Plan	TNCG works with our clients to develop a robust Continuity of Operations Plan (COOP) that delineates how a division or department will perform essential operations during an emergency or long-term disruption. It identifies mission-critical functions, communication methods, and alternate personnel, systems, and locations. Each department/division needs a COOP to ensure they can respond effectively in emergency situations.
Training and Exercises	TNCG assists our clients with training in the areas of emergency response, suspicious behavior indicators, and effective policies and procedures for security personnel. Training ranges from two-hour to all-day workshops. Formats for training include tabletop exercises, drills, and full-scale emergency response exercises.
Program Implementation	TNCG consultants will work with our clients on an ongoing basis to assist in the implementation of recommended mitigation strategies and the enhancement of security programs.
Technology Consulting	TNCG will provide our clients with technology assessments, programming, system design services, and specification development, bidding assistance, and full project management of implementation of systems.

Security Awareness Training

TNCG will conduct Suspicion Indicators Recognition and Assessment® (SIRA®) training that will focus on developing an increased level of security awareness for management and staff at the SPWRP plant facility. Training options will be determined after completion of the assessment. We offer the following options for this training:

1-Day, 8-Hour SIRA® Awareness Course

Course Description: The 8-Hour/1- Day Suspicion Indicators Recognition & Assessment awareness course is designed to increase awareness of pre-incident threat indicators for security and non-security personnel of any organization. This course will expose the participants to the current threat picture relevant to their organization and provide an overview of Security Interviewing and threat mitigation principles. Participants in this course will be aware of common pre-incident suspicion indicators and threat mitigation principles.

Learning Objectives:

- Learn Aggressors' Methods of Operation (AMOs).
- Learn Pre-Incident Suspicion Indicators.
- Practice Recognition of learned Suspicion Indicators.
- Learn Principles of Effective Security Interviewing & Threat Mitigation.

3-Day SIRA® Certification Course

Course Description: The 3-Day Suspicion Indicators Recognition & Assessment (SIRA®) course is designed to train participants to recognize pre-incident suspicion indicators on the field and have the basic ability to handle security interviews and apply proper threat classification and mitigation. Through practical exercises and in-class workshops, the 3-Day SIRA® course teaches security and law enforcement professionals to identify potential threats and resolve effectively or properly manage unresolved indicators through security interviewing and field operational protocols.

Learning Objectives:

- Understand Aggressors' Methods of Operation (AMOs).
- Practice proficiency in advanced recognition of pre-incident threat indicators.
- Learn to conduct Security Interviews.
- Develop a decision-making matrix to apply proper threat mitigation protocols.

5-Day SIRA® Certification Course

Course Description: The 5-Day/40-Hour SIRA® Certification is the most effective SIRA® course we offer. The instructors will hone in on participants' threat recognition skills, develop their proficiencies with field threat assessment, introduce Security Interviewing, and enhance their understanding and application of proven threat mitigation protocols.

Participants perform in-class workshops and dynamic field exercises and are required to pass a written and field examination. This ensures the participants are proficient and confident in applying the techniques effectively in their operational environments.

Learning Objectives:

- Enhance threat awareness.
- Participate in advanced field exercise as an aggressor.
- Practice detecting threat indicators in a realistic and dynamic environment.
- Learn how to conduct field threat assessments.
- Master conducting effective field security interviews.
- Practice applying proper threat mitigation protocols.

SIRA® THREAT INFORMATION PROTECTION SYSTEM

SIRA® THREAT INFORMATION PROTECTION SYSTEM (TIPS[sm]) is a proprietary software system that provides organizations with the tools and capabilities necessary to handle threat information proactively. This unique system conducts real-time trend analysis and generates an immediate alert on possible connections between current and previously reported suspicious activities, regardless of where, when, and by whom these activities were reported. This collaborative system enables the reporting field officer, management, and Analyst, to "connect the dots" between past and new suspicious activities across all clients' locations, thus increasing the ability to identify and address evolving threats in real time.

In addition to its analytical and alert features, TIPS provides subscribers with a comprehensive tool to report, log, track, and manage observed suspicious activities, threats, and other types of cases.

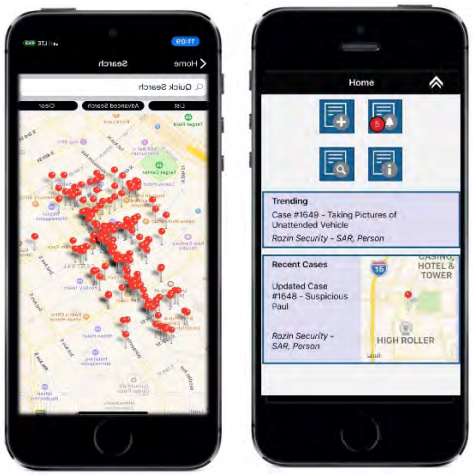


Exhibit 16 – Performance Measures

True North Consulting Group takes a proactive approach in Quality Control of their work product. As early as the development of schematic design, TNCG includes both internal and external peer reviews of drawings, specifications, and cost estimates.

TNCG follows industry standards for the Development of Technology Contract Documents (Drawings and Specifications) and adheres to methodologies refined and proven in the Design and Construction industries. These methodologies include a series of phases and milestone checklists for completion and coordination with other trades such as Architectural, Mechanical, and Electrical systems. TNCG's goal is to eliminate contractor additive change orders as a result of missing detail requirements in the Contract Documents.

Throughout the Contract Administration process, TNCG utilizes a combination of submittal reviews, field verification, and detailed checklists which have continually been developed to ensure that the Vendor(s) and Contractor(s) fully comply with the Contract Document requirements and that the Client receives the precise scope and quality for which they are paying.

True North Consulting Group's senior and most experienced staff members are integrally involved in quality control by applying years of experience and knowledge in the industry. TNCG is very proud that the majority of our clients have become repeat customers due to this high level of commitment to the quality of our work product, our professional services, and our ability to LISTEN to our clients.

Exhibit 15 – Options

Services Overview

DESCRIPTION OF SECURITY CONSULTING SERVICES PROVIDED BY TRUE NORTH CONSULTING GROUP	
Security Risk Assessments	Comprehensive, risk-based assessments of facilities and security programs utilizing DHS, FBI, and Israeli Shin Bet methodology. Assessments include risk analysis, threat assessment, vulnerability assessments, and mitigation recommendations. The goal of the assessment is to increase our client's ability to prevent, detect, deter, and respond to man-made threats to staff and visitors on facilities.
Threat Assessments	Comprehensive, community-specific threat assessments utilizing DHS and FBI methodology and incorporating up-to-date threat information from local and regional law enforcement, including regional FBI Fusion Center data and information.
CPTED Assessment and Mitigation	TNCG security and vulnerability assessments and mitigation recommendations include and address Crime Prevention Through Environmental Design (CPTED) principles.
Lighting Assessments	As part of our security assessments, TNCG will assess outside lighting levels for facilities and sites to ensure adequate levels of lighting for both prevention of threats as well as effective response to potential situations.
All-Hazards Mitigation	TNCG provides best practice all-hazard mitigation recommendations addressing based on security and vulnerability assessments. Mitigation recommendations are prioritized and address all three areas of security programs: physical, technology, and human factor security. Cost estimates are part of the mitigation recommendations if desired. Mitigation strategies are designed to address identified risks and threats.
Physical Security & Supporting Technology Infrastructure Design and Engineering, Acquisition & Project Management	True North provides these services in the following technologies: o Video Surveillance/CCTV o Identity Management o LAN (including Wireless LAN) o Access/Entry Control o Video Management Systems (VMS) o Video Analytics and Biometric Technologies o Alarm Systems/Intrusion Detection/Notification Systems o Communications/Dispatch Systems/Command Center
Security Master Planning	TNCG consultants provide security master planning services, providing our clients with a comprehensive, long-term strategy that covers all aspects of a security operation and provides sequential planning over a period of years to provide a safe, secure environment.

All-Hazards Emergency Management Planning	TNCG reviews emergency management plans, policies, and procedures, assists in updating plans and policies, and writes all-hazards emergency management plans for our clients. TNCG follows DHS and FEMA guidelines for emergency management planning, ensuring emergency management plans meet any local and state requirements.
Business Impact Analysis	TNCG assists clients in determining and evaluating the potential effects of an interruption to critical **business** operations as a result of a disaster, accident, or emergency, including IT functions.
Business Continuity Planning	With knowledge of the threats and risks faced by our clients, TNCG consultants work with them to create strategies and a plan to ensure that personnel and assets are protected and able to function in the event of an emergency both in the short-term and long-term.
Continuity of Operations Plan	TNCG works with our clients to develop a robust Continuity of Operations Plan (COOP) that delineates how a division or department will perform essential operations during an emergency or long-term disruption. It identifies mission-critical functions, communication methods, and alternate personnel, systems, and locations. Each department/division needs a COOP to ensure they can respond effectively in emergency situations.
Training and Exercises	TNCG assists our clients with training in the areas of emergency response, suspicious behavior indicators, and effective policies and procedures for security personnel. Training ranges from two-hour to all-day workshops. Formats for training include tabletop exercises, drills, and full-scale emergency response exercises.
Program Implementation	TNCG consultants will work with our clients on an ongoing basis to assist in the implementation of recommended mitigation strategies and the enhancement of security programs.
Technology Consulting	TNCG will provide our clients with technology assessments, programming, system design services, and specification development, bidding assistance, and full project management of implementation of systems.

Security Awareness Training

TNCG will conduct Suspicion Indicators Recognition and Assessment® (SIRA®) training that will focus on developing an increased level of security awareness for management and staff at the SPWRP plant facility. Training options will be determined after completion of the assessment. We offer the following options for this training:

1-Day, 8-Hour SIRA® Awareness Course

Course Description: The 8-Hour/1- Day Suspicion Indicators Recognition & Assessment awareness course is designed to increase awareness of pre-incident threat indicators for security and non-security personnel of any organization. This course will expose the participants to the current threat picture relevant to their organization and provide an overview of Security Interviewing and threat mitigation principles. Participants in this course will be aware of common pre-incident suspicion indicators and threat mitigation principles.

Learning Objectives:

- Learn Aggressors' Methods of Operation (AMOs).
- Learn Pre-Incident Suspicion Indicators.
- Practice Recognition of learned Suspicion Indicators.
- Learn Principles of Effective Security Interviewing & Threat Mitigation.

3-Day SIRA® Certification Course

Course Description: The 3-Day Suspicion Indicators Recognition & Assessment (SIRA®) course is designed to train participants to recognize pre-incident suspicion indicators on the field and have the basic ability to handle security interviews and apply proper threat classification and mitigation. Through practical exercises and in-class workshops, the 3-Day SIRA® course teaches security and law enforcement professionals to identify potential threats and resolve effectively or properly manage unresolved indicators through security interviewing and field operational protocols.

Learning Objectives:

- Understand Aggressors' Methods of Operation (AMOs).
- Practice proficiency in advanced recognition of pre-incident threat indicators.
- Learn to conduct Security Interviews.
- Develop a decision-making matrix to apply proper threat mitigation protocols.

5-Day SIRA® Certification Course

Course Description: The 5-Day/40-Hour SIRA® Certification is the most effective SIRA® course we offer. The instructors will hone in on participants' threat recognition skills, develop their proficiencies with field threat assessment, introduce Security Interviewing, and enhance their understanding and application of proven threat mitigation protocols.

Participants perform in-class workshops and dynamic field exercises and are required to pass a written and field examination. This ensures the participants are proficient and confident in applying the techniques effectively in their operational environments.

Learning Objectives:

- Enhance threat awareness.
- Participate in advanced field exercise as an aggressor.
- Practice detecting threat indicators in a realistic and dynamic environment.
- Learn how to conduct field threat assessments.
- Master conducting effective field security interviews.
- Practice applying proper threat mitigation protocols.

SIRA® THREAT INFORMATION PROTECTION SYSTEM

SIRA® THREAT INFORMATION PROTECTION SYSTEM (TIPS[sm]) is a proprietary software system that provides organizations with the tools and capabilities necessary to handle threat information proactively. This unique system conducts real-time trend analysis and generates an immediate alert on possible connections between current and previously reported suspicious activities, regardless of where, when, and by whom these activities were reported. This collaborative system enables the reporting field officer, management, and Analyst, to "connect the dots" between past and new suspicious activities across all clients' locations, thus increasing the ability to identify and address evolving threats in real time.

In addition to its analytical and alert features, TIPS provides subscribers with a comprehensive tool to report, log, track, and manage observed suspicious activities, threats, and other types of cases.

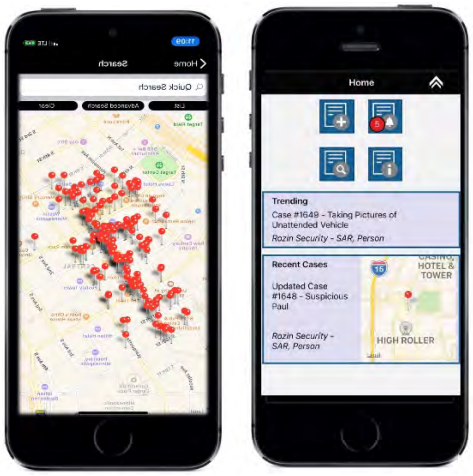


Exhibit 16 – Performance Measures

True North Consulting Group takes a proactive approach in Quality Control of their work product. As early as the development of schematic design, TNCG includes both internal and external peer reviews of drawings, specifications, and cost estimates.

TNCG follows industry standards for the Development of Technology Contract Documents (Drawings and Specifications) and adheres to methodologies refined and proven in the Design and Construction industries. These methodologies include a series of phases and milestone checklists for completion and coordination with other trades such as Architectural, Mechanical, and Electrical systems. TNCG's goal is to eliminate contractor additive change orders as a result of missing detail requirements in the Contract Documents.

Throughout the Contract Administration process, TNCG utilizes a combination of submittal reviews, field verification, and detailed checklists which have continually been developed to ensure that the Vendor(s) and Contractor(s) fully comply with the Contract Document requirements and that the Client receives the precise scope and quality for which they are paying.

True North Consulting Group's senior and most experienced staff members are integrally involved in quality control by applying years of experience and knowledge in the industry. TNCG is very proud that the majority of our clients have become repeat customers due to this high level of commitment to the quality of our work product, our professional services, and our ability to LISTEN to our clients.

Exhibit 17 – Addendums

Please see TNCG's completed and signed Addenda on the following pages.

DAS
Iowa Department of Administrative Services
Service • Efficiency • Value

Governor Kim Reynolds
Lt. Governor Adam Gregg
Paul Trombino III, Interim Director

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

04-28-2020
Date

Ron Bundy
Typed or Printed Name

DAS
Iowa Department of Administrative Services
Service • Efficiency • Value
Governor Kim Reynolds
Lt. Governor Adam Gregg
Paul Trombino III, Interim Director

April 13, 2020

To: All Potential Respondents
From: Randy Worstell, Purchasing Agent
Subject: RFP0920005016

Addendum Two

Please amend the subject RFP to include answers to the following timely received questions:

Q1. Would you be able to provide more information regarding the scope of work for this project? Information pertaining the type of operation, number and sq. of facilities, as well as desired completion time would aid in providing you with a more accurate estimation of cost and a detailed approach. **but we did not see one provided in the RFP. Is this something we just create?**

A1. This is a general RFP to identify qualified and pre-selected suppliers to place on Master Agreements for Security Assessment and Design Services. State Agencies and Department will contact selected supplier with a Scope of Work and Timeline when a need for assessment or design service arise. If you would like to provide a Request for Service template

Q2. Given the challenges of the pandemic, may additional time be granted for our solicitation. Our workforce is presently working remotely under social distancing recommendations.

A2. Addendum One pushed the Response Due Date to April 30, 2020 @ 1:00 P.M. central time. This is being monitored to determine if another delay maybe considered.

Q3. Does the state have an incumbent presently?

A3. No

Q4. Is in-state consultant desired?

A4. Covered in Section 2.28

Q5. Does the state have standardized documentation for security systems or is this all performance based, and will need to be created by consultant?

A5. This will be performance based, and will need to be created by consultant?

Hoover State Office Building 1305 East Walnut Street Des Moines, IA 50319 (515) 281-5360 http://das.iowa.gov

Q6. What is the expected value of tasks?

A6. Unable to determine value at this time,

Q7. Is this solely for hourly rates? If individual asks are to be procured, can we obtain additional scope details?

A7. This proposal is requesting hourly rates by positions, if you have a different pricing model please include along with the hourly rates.

Q8. Is there a break out of assessment/design anticipated? Can a percentage allotment be provided?

A8. Since the contract will be open to all State Agency and Political Subdivisions there is no way of anticipate the break out between assessment vs design.

Q9. What is the average building size that may require assessment or design services?

A9. Since the contract will be open to all State Agency and Political Subdivisions there is no way of determining average building size/type or location.

Q10. What building types may require these services?

A10. Mainly Office Complexes and/or Warehouses, but other types are possible.

Q11. Is there a general location, or will it be across the state?

A11. Current need is within the Capital Complex located in Des Moines, IA but the Master Agreement is anticipated to be open State Wide

Q12. Are hazardous conditions anticipated?

A12. No hazardous condition expected.

Q13. Are assessments to include operational reviews? Emergency preparedness? Policies, procedures?

A13. No, not part of this scope

Q14. What is the expected amount of work? For instance, how many consulting tasks are anticipated in a year?

A14. Undetermined at this time.

Q15. Will the consultant be required to develop door hardware schedules?

A15. This depends on the site requesting the assessment.

Q16. Are electrical, mechanical, telecommunication, fire alarm design services also envisioned?

A16. Not include in the scope of this Master Agreement.

Q17. Will vendors be allowed to bid? Is service independence required? I.e. (security guard companies cannot participate.)

A17. Section 4.1.11 and 4.2.8 refence "Respondent shall not be in the business of selling security systems hardware" service independence is required.

Q18. Will we prepare design and provide to state for bid administration?

A18. Yes, we will be asked to provide designs and specification/recommendations for equipment, the State will be responsible for preparing any bid documents.

Q19. Sample reports are required. We would suggest a table of contents. Reports are confidential and cannot be released. If shortlisted, we could provide a review of a report in person, but not digitally. Is this acceptable?

A19. We are asking for a "Mock" report, please DO NOT include any customer information.

Q20. Please further define cash discount. Are you proposing to pay us in cash directly?

A20. The State of Iowa standard Payment Terms is Net 60 days, the question refers to any discount the supplier might offer for early payment (Example: 2% discount for payment in 15 days).

Q21. Must all team member have staff that are certified, or is only the Project Manager required to hold this certification?

A21. It's find if only the Project Manager holds the certification.

Q22. Regarding the following statement:" Respondent must have the ability to perform security assessment of State of Iowa facilities and/or Subs." What is meant by the statement "/or Subs?"

A22. The term "Subs" means the Master Agreement would be open for Municipalities, City, Counties and School Districts in the State of Iowa to participate in at the contracted pricing.

Q23. Please define the term "respond" with regards to the following statement: "Respondent shall respond to assessment request within 48 hours.".

- Does this mean respond and schedule or does this mean be on-site and begin assessment?

A23. This means the selected respondent would have 48 hours to acknowledge the receipt of an Assessment or Design request and begin discussion with requestor on timeframe and scope of work.

Q24. Regarding the statement, "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". can the following be added: unless legally obligated to do so.

A24. Yes, we can include the suggested change.

Q25. Minus element identified, is there any other scoring criteria? Is this a cost driven exercise?

A25. The scoring elements and scoring criteria will be posted prior to bid closing.

Q26. Has a budget been allocated for FY20/21?

A26. No

Q27. Can you provide any insight on the historical scope of this type of service in the past few years? How many separate projects?

A27 This type of work has never been performed under a Master Agreement for the State of Iowa in the past. There may have been Agency/Department specific projects in the past

Q28. On page 17, paragraph 4.1.9 of the RFP, the State calls for a 48-hour response to an assessment request. Will the State accept a phone call or e-mail as a response to a request?

A28 Same Question 23, please see A23.

Q29. Does the State have a target number of assessments being completed each year?

A29 Undetermined at this time.

Q30. Does the State have an incumbent contractor conducting security assessments?

A30. No

Q31. What is the size of the largest facility and the smallest facility the state will require security assessments to be completed?

A31 Unable to determine at this time, State of Iowa has 17 Agencies 27 Facilities and 85 Building and approx. 185 leases.

Q32 On page 14, Exhibit 13 – Security Systems Design Service of the RFP, the fifth bullet statement reads: "Provide an estimate of **State of Iowa** staff time required to complete the Security System Design if different then Exhibit 11."
Should the fifth bullet statement be changed to read:
Provide an estimate of **Respondent** staff time required to complete the Security System Design if different then Exhibit 11?

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 <u>return this letter with your offer (do not send back separately).</u>

I hereby acknowledge receipt of this addendum.

Ron Bundy

Signature

04-28-2020

Date

Ron Bundy

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

04-29-2020
Date

Ron Bundy
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.***

True North Consulting Group, LLC.	RFB0920005016	Security Assessment & Design Services
Company	RFP Number	RFP Title
Signature (required)	Sr. Strategy Consultant	04-28-2020
	Title	Date

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

Part 2 - Confidential Treatment is Requested

The below information is to be completed and signed ONLY if Respondent is requesting confidential treatment of any information submitted in its Proposal.

NOTE:
- ***Completion of this Form is the sole means of requesting confidential treatment.***
- ***A RESPONDENT MAY NOT REQUEST PRICING INFORMATION BE HELD IN CONFIDENCE.***

Completion of the Form and Agency's acceptance of Respondent's submission does not guarantee the agency will grant Respondent's request for confidentiality. The Agency may reject Respondent's Proposal entirely in the event Respondent requests confidentiality and does not submit a fully completed Form or requests confidentiality for portions of its Proposal that are improper under the RFP
.

Please provide the information in the table below. Respondent may add additional lines if necessary or add additional pages using the same format as the table below.

RFP Section:	Respondent must cite the specific grounds in *Iowa Code Chapter 22* or other applicable law which supports treatment of the information as confidential.	Respondent must justify why the information should be kept in confidence.	Respondent must explain why disclosure of the information would not be in the best interest of the public.	Respondent must provide the name, address, telephone, and email for the person at Respondent's organization authorized to respond to inquiries by the Agency concerning the status of confidential information.

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. A copy of this document shall be placed in all Proposals submitted including the Public Copy.

- ***If confidentiality is requested, failure to provide the information required on this Form may result in rejection of Respondent's submittal to request confidentiality or rejection of the Proposal as being non-responsive.***

- ***Please note that this Form is to be completed and signed only if you are submitting a request for confidential treatment of any information submitted in your Proposal. If signing this Part 2, do not complete Part 1.***

_____	RFB0920005016	Security Assessment & Design Services
Company	RFP Number	RFP Title
_____	_____	_____
Signature (required)	Title	Date