⊙INA

Proposal for

Security Risk Assessment

Prepared Exclusively For
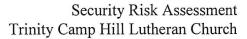
trinity | camp hill
LUTHERAN CHURCH

Prepared by

Information Network Associates, Inc.

5235 North Front Street
Harrisburg, PA 17110
(717) 599-5505
Fax: (717) 599-5507
www.ina-inc.com

September 1, 2022

September 1, 2022

Pastor Jack Horner
Trinity Evangelical Lutheran Church
2000 Chestnut Street
Camp Hill, PA 17011

Re: Security Risk Assessment

Dear Pastor Horner,

Pursuant to our recent conversation, Information Network Associates, Inc. (INA) is pleased to submit for your review and consideration the following proposal for a security risk assessment survey for the Trinity Evangelical Lutheran Church (TELC)
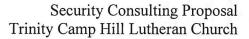
INA is a thirty-five year leader in the field of professional security consulting. Our team of security professionals has the experience and expertise and resources to assist TELC in providing a safer environment for its staff, parishioners and visitors. INA has extensive experience in conducting security risk assessments for government, corporate, houses of worship and educational institutions around the world. Our clients include 20 percent of Fortune 100 Companies. INA also has considerable knowledge of houses of worship security best practices and benchmarks.

Scope and Objective

INA proposes to perform security consulting services to identify and mitigate risk to the TELC. The services proposed will include risk analysis and physical security assessment of the Church, its administrative offices, and grounds.

The overall objectives of this project will be to:

1. Identify existing physical security measures that can be exploited by others or that create vulnerabilities and increase risk to staff, parishioners and visitors

2. Evaluate current policies, procedures, and security related operations;

3. Identify the role of church personnel and parishioners during an emergency;

4. Identify resources available to church personnel during an emergency.

5. Evaluate the use and effectiveness of electronic security systems, including access control, video systems, intrusion detection, panic buttons, and other electro-mechanical devices;

6. Evaluate the internal and external threats that affect the churches security profile;

7. Review various practices and written procedures, including pre-employment screening, crisis management, business continuity, workplace violence, demonstration action, media relations, and threat assessment, bullying, and crisis management;

8. Evaluate present and future implications of safety and security measures presently in effect and to be proposed;

9. Provide recommendations / options for consideration to provide a safer and more secure environment.

INA will document all of its findings in a comprehensive written report that will provide recommendations / options for consideration. The scope of this project is limited and will not include IT security, penetration testing, regulatory compliance, or OSHA compliance.

Technical Approach and Work Plan

INA proposes to accomplish the outlined objectives through the following technical approach and work plan:

Step I – Perform a Threat Analysis
Generally, an effective security program must be designed to combat any type of situation that threatens the well-being of life and property. Therefore, the first step in the survey is to determine the nature and extent of the threats, existing and anticipated, internal and external. While all public institutions have common threats, each property has unique issues. These concerns will vary in degree of risk and vulnerability to various factors, including, but not necessarily limited to, geographic location, building design, exposure of key personnel or leaders, local crime rate, police response /community cooperation, and security culture,

Step II – Perform a Physical Risk/Vulnerability Evaluation
The next step will be to conduct an in-depth physical survey of the buildings and property. The effectiveness of any current physical and electronic security systems/programs and security guard operations (if applicable) will be evaluated. The information developed in the initial phases will provide direction toward certain areas of concern and enable the survey team to formulate meaningful recommendations for security hardware and procedural needs compatible with company philosophy. This task includes, but is not limited to, an examination of the following, as appropriate:

1. Building grounds security

2. Interior building security

3. Electronic security systems (alarm, CCTV, access control, etc.)

4. Lighting

5. Access control systems

6. Control of authorized entry and movement

7. Visitor and vendor controls

8. Signage

9. Lock and key control

10. Safes and vaults

11. Identification card procedures

12. Background security checks

13. Incidents/incident reporting

14. Emergency, contingency evacuation

15. Incident reporting system

16. Security forces and equipment

17. Communications systems

18. Emergency policies and procedures

19. Protection of utilities

20. Fire evacuation procedures

21. Lockdown procedures

22. Disaster recovery plan

23. Overall preparedness

24. Staff training

Photographs will be taken during the site visit and will be incorporated and referenced in the final report.

NOTE: The site surveys specifically exclude life safety measures (OSHA or similar agency), hazmat handling and storage, environmental protection matters, or government building codes and mandates.

Step III – Conduct a Site Survey

The next task includes conducting structured interviews with selected individuals to include Pastor Horner and Steve Kauffman. Based on prior experience, we anticipate the following types of information will be developed from our discussions:

1. Perception of the effectiveness of security procedures, physical security measures, and internal security controls in effect;

2. Perception of internal and external threats;

3. Perception of the security environment such as problems, concerns, and vulnerability;

4. Contingency planning for unusual events, such as; natural and man-made disasters, property destruction, bomb threats, unwanted intruders, etc.;

5. Police, fire, and medical response capability;

6. Incident report procedures and analysis;

7. Security awareness programs;

8. Security training requirements and efficiency;

9. Administrative staff capability to assess and evaluate threats;

10. Liability issues;

Step IV – Formulate Recommendations / Options for Consideration

Based on an analysis of the findings, specific recommendations for overall risk management will be provided. Recommendations will be prioritized by perceived risk to the organization. Many options for consideration will not cost anything and may require simple changes to practices, policies, or procedures. Other items may be budgeted for and implemented over time as funding permits. Planned construction, acquisition, or projects will also be evaluated and incorporated.

Step V – Implement the Recommendations

The effectiveness of any reasonable security program ultimately depends on how thoroughly professional recommendations are implemented and practiced. While implementation is beyond the scope of this proposal, INA will work with and continue to be a resource to the TELC to assist in implementing the recommendations set forth in our report.

Methodology

INA views security not as a discipline with its own body of knowledge, but as a field that utilizes concepts, hypotheses, and propositions from many disciplines. For this reason, in our judgment, each project requires the collective expertise of security professionals possessing the requisite multi-disciplinary skills indicated by the specifics of the assignment. Further, we believe security programs must be based on the anticipation criminal activity will inevitably occur and security systems must be designed and implemented that will deter, thwart, or impede those acts. As such, INA does not represent its findings and recommendations alone represent the basis for an absolute crime resistant security program.

It is INA's policy to maintain continuous interface with designated staff since experience has shown in projects of this nature a development of a close working relationship is necessary to ensure a viable and meaningful end product. Lastly, it is also our practice to bring any significant findings to your immediate attention.

Compensation and Terms

INA's fee for completing these risk assessment surveys as outline in this proposal is $2,500.00. INA will accept a purchase order or written authorization of acceptance from the TELC in an email or letter as approval of the terms in this document. TELC will be invoiced at the conclusion of the project upon delivery of the final report. The payment terms will be NET 30 days.

INA will also assist with developing written policies and procedures on security related areas at an hourly cost of $50.00 per hour with a budget not to exceed $1000.00 without the approval of the client. Policy writing is separate from the Security Risk Assessment.

INA will provide training to the TELC in-house security team at an hourly cost of $50.00 with a budget not to exceed $1000.00 without the approval of the client.

INA will provide Armed or unarmed security services at the following hourly rates:
Armed security rate: $41.00
Unarmed security rate: $38.00

Timeline

INA will begin the security assessment research immediately upon acceptance of the proposal. The on-sight security review will be scheduled upon written approval. It is anticipated the site visit will require one to two days onsite. Designated personnel will need to be available for interviews during these dates. Follow up phone interviews may be required for unavailable personnel. Verbal recommendations would be provided immediately after the onsite inspection and the final written report will be completed within thirty days after the site visit or follow up interviews.

Please contact me if you have any questions regarding this statement or if you require any supplemental information. We sincerely appreciate the opportunity to provide this information to you, and we thank you for considering INA to fulfill your security consulting requirements.

I look forward to working with you on this project to help accomplish the goal of maintaining a safe and secure environment for Trinity Camp Hill Lutheran Church.

Sincerely,
Information Network Associates, Inc.

Richard W. Carpenter
Vice President

THE PARTIES HAVE READ THIS AGREEMENT, UNDERSTAND IT, AND BY SIGNING BELOW AGREE TO BE BOUND BY IT. EACH PARTY REPRESENTS THAT THE INDIVIDUAL SIGNING ON ITS BEHALF HAS FULL AUTHORITY TO BIND SUCH PARTY.

ACKNOWLEDGED AND AGREED TO:

By: _____
(Trinity Camp Hill Lutheran Church)

By: _____
(Information Network Associates)

Printed Name: _____

Printed Name: _____

Title: _____

Title: _____

Date: _____

Date: _____