A PROPOSAL TO

Village of Orland Park

NIST SP 800-82 SCADA\OT Assessment

NOVEMBER 20, 2025

SENTINEL®

TABLE OF CONTENTS

General Contact Information

SENTINEL CONTACT INFORMATION

Ryan Aubin
Sales Executive
2550 Warrenville Rd., Downers Grove, IL 60515
630.786.8403 fax 630.769.1399
raubin@sentinel.com

Environmental Policy Statement

At Sentinel, environmental protection is a management responsibility as well as the responsibility of every employee. Our environmental protection policy addresses all aspects of the corporation's operations which can potentially impact the environment. In creating this policy, we have taken into account the following factors:

- Compliance with applicable laws, regulations, and standards concerning environmental protection
- Establish corporate environmental objectives and targets
- Minimize the environmental risks to our employees and the communities in which we operate
- Promote employee awareness of environmental concerns, actions, and responsibilities
- The efficient use of energy and materials in our operations
- Reduce/ eliminate waste through recycling and responsible disposal
- Continuous improvement and monitoring of the current environmental policy

Further, Sentinel suppliers are encouraged to develop an Environmental Policy and Environmental Management System by following the Environmental Protection Agency guidelines.

SSAE 16 SOC 2, Type II Attestation

Standing at the apex of Sentinel's myriad awards, honors and certifications is its SSAE 16 Service Organization Control (SOC) 2, Type II Attestation which has been undertaken annually by the nationally-renowned auditing firm Plante Moran, PLLC for the past three years. The SOC 2, Type II attestation is the highest and most rigorous in the SSAE 16 portfolio of audits, evaluating Controls and Processes that encompass the Five Trust Service Principles of Security, Availability, Processing Integrity, Confidentiality and Privacy.

Why should this matter to you? The SSAE 16 attestation provides independent validation and assurance that Sentinel is in compliance with best practices regarding items of critical importance to you -- security, confidentiality, data protection, project management and IT strategic solutions, to name a few. If you are seeking consulting or services support for your IT environment, the SOC 2, Type II attestation should be one of the most important factors in your evaluation.

The SSAE 16 Attestation is a standard that was created by the American Institute of Certified Public Accountants (AICPA) in 2010 to replace the SAS 70 certification process, and expand reporting to the effectiveness of a service organization's controls relating to operations and compliance.

Executive Summary

Village of Orland Park has engaged Sentinel to provide a National Institute of Standards and Technology (NIST) Cybersecurity assessment (NIST SP 800-82 Rev. 3) of the current cybersecurity infrastructure and provide recommendations that are based on a strategic approach.

The strategic assessment approach aligns organizational goals and objectives with technology recommendations. Sentinel will meet with key organization stakeholders to gain insight into current challenges as well as future initiatives. This process will provide guidance for the analysis and recommendation phases of the engagement. Sentinel will gather information about the current cybersecurity infrastructure, topology, devices, and configuration to review it for best practice adherence and alignment with the NIST SP 800-82 standard. A prioritized list of recommendations will be presented to the organization and linked to the key initiatives that are defined in prior phases. The goal of the assessment is to provide a comprehensive analysis and objective review of the current cybersecurity posture and provide insight into any future changes that should be made.

As a follow-up to the assessment engagement, Sentinel can provide remediation services for those objectives the Customer wishes to pursue and remediate further. Sentinel appreciates the opportunity to provide these services to Village of Orland Park and looks forward to reviewing the results with the team.

This engagement will include two locations and review of collected packet captures through an OT security tool, Cisco Cyber Vision. Sentinel engineers may assist Village of Orland Park in collecting these packet captures and maintaining security of these packet captures.

Assessment Services Overview

Heading 2

HEADING 3

Heading 4

Font – Times New Roman 10.5

Phase One - Information Gathering

- The first phase of the assessment is an information gathering engagement that will provide detailed information about the current environment including both technical and non-technical data. For strategic assessments, Sentinel will meet with the Customer stakeholders through an interview session to gather key objectives and goals for the organization. This information will be used to provide perspective and influence on the analysis and recommendations in later phases of the assessment.

- A solid security plan goes beyond technology and addresses the entire cybersecurity lifecycle of an organization. A Sentinel Strategic Advisor will review the NIST SP 800-82 Framework with the Customer and review organizational alignment to these standards. The NIST SP 800-82 framework provides a comprehensive approach to protecting critical infrastructure using standards and guidelines.

During this phase, Sentinel engineers will assist in collecting packet captures of the two locations. These packet captures will be processed through Cisco Cyber Vision to get an understanding of the OT network.

Phase Two - Analysis

The second phase of the assessment includes a thorough analysis of the collected information from phase one and performs a technical gap analysis between the current implementation and a best practice implementation in several categories.

The strategic analysis identifies actionable items that factor into the Customer's organizational requirements, objectives, and goals. This option allows the recommendations to be tailored for the Customer, providing influence and perspective in other areas such as growth, performance, and resiliency, using a holistic approach to ensure the most reliable and functional environment possible. Stakeholder interviews will be performed during the information discovery phase to identify the goals and objectives that will influence the analysis and subsequent recommendations in the final phase of the assessment. Sentinel will work with the Customer to help identify any gaps between the current organizational security approach and those defined by NIST and industry best practices.

Phase Three – Recommendations

- The third phase of the assessment is where Sentinel will provide a prioritized list of recommendations based on the analysis performed during phase two of the assessment. The strategic assessment recommendations will be influenced and evaluated based on Customer organizational goals and

objectives gathered during phase one. Findings will be prioritized based on business impact, likelihood, and risk, to determine overall priority.

- Sentinel services during this phase may include, but are not limited to the following:

- Strategic Assessments.
    - Organizational alignment to goals and future state objectives.
    - Overall constraints, budgets, non-technical influences.
    - Security deficiency identification with recommendations.
    - Software/hardware upgrade recommendations.

Scope of Work

Phase One – Information Gathering

PROCESS

- Strategic Assessments.
    - Sentinel will work with the customer to determine the appropriate stakeholders that will be interviewed.
    - Sentinel will provide the customer with a pre-interview overview of the question topic areas so that stakeholders can be properly prepared.
    - Sentinel will perform an interview session with key customer stakeholders to gather information regarding organizational goals and objectives.
    - Sentinel will review the items within scope for the assessment with the customer to ensure agreement and any additional information, comments, or concerns about the environment.
    - Review the NIST SP 800-82 Framework and Customer cybersecurity policies and procedures.
    - Sentinel will perform remote data collection on the infrastructure components considered in scope for the respective technology areas. This may include applications, devices, services, etc. depending on the environment.
    - Perform packet captures on the OT network to be processed and analyzed by Cisco Cyber Vision.

SENTINEL DELIVERABLES

- Strategic Assessments.
    - Stakeholder information gathered during interview sessions.
    - Review of alignment score and required evidence

CUSTOMER RESPONSIBILITIES

- Strategic Assessments.
    - Determine appropriate organization stakeholders that should participate in the stakeholder interview sessions. This will include both technical and non-technical participants.
    - Provide employee list and contact information.
    - Participate in stakeholder meetings to gather appropriate organizational information.
    - Participate in meetings to review documentation results.
    - Access to network switches in OT environment
    - Ability to configure port spanning as necessary

Phase Two - Analysis

PROCESS

- Strategic Assessment.
    - This includes a broader conversation around the infrastructure as a whole and includes a deeper analysis of the Customer requirements based on organizational goals.
    - Sentinel will document recommendations and tailor them to meet the Customer's identified goals and objectives where applicable. O
    - A broader in Scope conversation around the NIST SP 800-82 Framework will be performed as well as a deeper analysis of the Customer's security posture.
    - Sentinel will review collected policies and procedures and identify areas of improvement and/or compliance concerns.
    - Process the packet captures through Cisco Cyber Vision to identify all systems on the OT networks and analyze device software levels and vulnerabilities.

SENTINEL DELIVERABLES

- Sentinel will provide a summary of the analysis findings in a prioritized listing. This document will identify gaps that were observed during the information-gathering and analysis phases of the assessment. This information will be used to develop the prioritized list of recommendations for the infrastructure under assessment. Priority will be weighted based on compliance requirements and industry practices.
    - Stakeholder interview session goals and objectives summary.
    - Technology alignment with the organizational direction and focus.
    - Future project impact, timelines, milestones, and goals.

CUSTOMER RESPONSIBILITIES

- Participate in any meetings to review documented findings.

Phase Three – Recommendations

PROCESS

- Sentinel will utilize the findings from the analysis phase to provide a prioritized list of recommendations.
- Each recommendation will include background information on the topic being discussed in order to provide context for the technical recommendation to follow. Recommendations may reference industry or manufacturer best practice documentation as well as suggested high-level remediation steps.
- Supplemental documentation may be provided for customer reference and additional supporting documentation relating to NIST SP 800-82.
- Provide documentation on Cisco Cyber Vision analysis.

SENTINEL DELIVERABLES

- Sentinel will provide a prioritized list of recommendations to the customer based on the analysis findings.
- Sentinel will build a Plan of Action and Milestones
- Sentinel will build a System Security Plan

CUSTOMER RESPONSIBILITIES

- Participate in meetings to review documented recommendations.

Project Management

- Sentinel will provide a project manager committed to the success of the project. The project manager will be responsible for:
- Complete success of the project.
- Optimal coordination of all resources.
- Guiding the customer on aspects of the project they are required to perform.
- Tracking and reporting of progress.
- Management of expected timelines for the assessment.
- Changes to the project and communications of changes in writing using a Change Order form.
- Post-assessment project completion agreement and signature.

Project management will ensure complete project success. Communication is the cornerstone of project management, and the project manager will be the central communication mechanism for all parties. This will ensure all relevant parties are informed about decisions that may affect the success of their component of the solution.

General Assumptions

- The following is a list of general project assumptions which Sentinel assumes have been completed or reviewed by the customer prior to the start of the project.
- Sentinel guarantees that it will perform any tests responsibly and professionally, following best practices. It will use its best efforts not to change or amend any applications, data, programs, or components of the Customer's network (including hardware and software). It does not guarantee any disruption or effect on the Customer's production systems. The Customer understands that Sentinel shall not be liable for any damages that may arise from any such interruption.
- The current infrastructure under assessment is in an operational state, excluding any specific issues that may be under evaluation as part of the assessment services. Sentinel has not included any troubleshooting or remediation services as part of this proposal.

- The Customer has access to all infrastructure areas under assessment and can provide this information to Sentinel. Note: Service provider managed equipment may not be accessible and therefore excluded from assessment unless configuration(s) can be provided by the customer.
- For strategic engagements, the stakeholder interview sessions may be performed via WebEx or MS Teams.
- Any information discussed and/or provided by Sentinel to the customer is considered confidential and should not be distributed outside the customer's organization without Sentinel's written approval.
- Sentinel will not be making system configuration changes during this engagement. If these needs are identified, a separate proposal will be created for that work.
- Generally, services are quoted at a standard rate for labor from 9:00 a.m. – 5:00 p.m. If Customer requires, Contractor can perform some of these services outside of normal business hours at an overtime labor rate.
- Travel and expenses are not included in the pricing and are billed to the Customer as actuals.