

Security System Services



SecureState

Request for Proposal (RFP)

3/26/2015

Version 1.0



TABLE OF CONTENTS

1	INTRODUCTION.....	3
1.1	PURPOSE	3
1.2	OVERVIEW OF SECURESTATE.....	3
1.3	SCHEDULE.....	3
1.4	CONFIDENTIALITY.....	3
2	SUBMISSION GUIDELINES.....	3
2.1	PROPOSAL ORGANIZATION	4
2.1.1	<i>Section 1: Company Overview.....</i>	<i>4</i>
2.1.2	<i>Section 2: Implementation Methodology.....</i>	<i>5</i>
2.1.3	<i>Section 3: Pricing.....</i>	<i>5</i>
3	STATEMENT OF WORK.....	5
3.1	SCOPE.....	5



1 Introduction

1.1 Purpose

SecureState requires upgrades to its existing security system to meet our growing security needs. This includes replacement of, or upgrades to, our existing Card Readers, Cameras, and Alarm Systems.

1.2 Overview of SecureState

SecureState is a leading provider of innovative security services and solutions for commercial and government clients. From its beginning in 2001, SecureState consistently has delivered innovative information technology and technical services solutions to its clients. Our expertise covers enterprise security architecture, information assurance, software development, intelligence operations support, network and critical infrastructure protection, and information technology support.

1.3 Schedule

While subject to change, the following is the anticipated project schedule for the evaluation.

3/26/2015	Issue Request for Proposal
4/9/2015	Questions on RFP due by 5:00pm EST to securityRFP@securestate.com
4/16/2015	Response to vendor questions released
4/30/2015	RFP response submissions due via email by 5:00pm EST
5/1/2015 – 5/21/2015	Review RFP Responses and Conduct Vendor Interviews
5/21/2015 (approximate)	Vendor selection and notification of award

1.4 Confidentiality

All response materials will be held in the strictest confidence. Only those participating in the evaluation process will have direct access to the response materials.

SecureState considers the response from the chosen vendor to be the precursor to a formal contract(s). All of the statements and information contained in the response are considered to be a true and accurate representation of the vendor's capability.

In the event that a formal Non-Disclosure Agreement (NDA) is required as a precursor to the response submission, the NDA must be submitted to SecureState by 4/23/2015. SecureState will not accept any delays in the execution of the NDA as a justification for missing the submission deadline.

2 Submission Guidelines

Electronic copies of the proposal response and any questions should be emailed to the contact below:

Chris Makley, Network Administrator
securityRFP@securestate.com

Your response must be received by end of business (5:00 PM EST) on April 30, 2015. Any response received after the deadline will not be considered.



2.1 Proposal Organization

The format for the response to this RFP should be in three sections with supporting documentation and appendices.

- Section 1: Company Overview
- Section 2: Implementation Methodology
- Section 3: Pricing

2.1.1 Section 1: Company Overview

This section should contain responses to each of the items listed below. The response should be sufficient to convey your level of knowledge and experience. This section should also contain any information that does not fit within the remaining parts but you feel is important to differentiate your offering. Any supporting materials may be submitted as an appendix

Items to Address:

- **COMPANY BACKGROUND** - Provide a brief description of your company's history. If applicable, provide any parent/subsidiary arrangements and the primary ownership of these organizations.
- **CORPORATE SIZE** - Describe your company in terms of its employees. Provide the number of total employees as well as the number of employees that could be used to support, directly and indirectly, SecureState's requirements.
- **SERVICING AND SUPPORT OF SYSTEM** – Describe how your company services and supports integrated systems you install. What are standards SLAs on services calls? Is service and support performed solely by in-house resources or are 3rd parties/subcontractors used? If you leverage 3rd party/subcontractors for system servicing and support how do you ensure quality standards are meet?
- **CENTRAL MONITORING** –Describe your capabilities to provide security monitoring. Specifically list:
 - If central monitoring is performed in-house or relies on subcontractor/third parties
 - If central monitoring supports 24x7x365 monitoring with failover and redundancy
 - If monitoring failover and redundancy is performed in-house or by a subcontractor/third party
 - Any pertinent certifications of the central monitoring facility
- **CORPORATE CERTIFICATIONS** – Provide a current list of ACS you are certified to install and integrate. Provide a current list of VMS you are currently certified to install and integrate.
- **CORPORATE BONDING AND INSURANCE COVERAGE** – Describe your company's bonding and insurance coverage as it relates to this project.
- **CORPORATE EXPERIENCE** - Your response should indicate your capability and actual experience, including your capabilities in the following areas:
 - Years performing similar work
 - Average installs performed per year
- **REFERENCES** – Provide three references for projects of similar scope, size, and complexity



2.1.2 Section 2: Implementation Methodology

The purpose of this section is to obtain information on the methodology that would be used to achieve the goals of this project. The following **Section 2: Statement of Work** outlines the scope of the new system and specific requirements the system and System Integration team will need to address.

For SecureState to effectively analyze the information provided by the various vendors, certain key aspects of their approach must be provided. The following list provides the key points that should be addressed by your methodology for each of the tasks outlined in the SOW:

- **APPROACH** - Outline the techniques used to successfully execute this. Outline the deliverables and/or outcomes of the steps.
- **RESOURCES** – Define the resources required for each major task.
- **QUALITY CONTROL** – Define the quality control processes used to ensure the above major tasks are completed to design specifications and client needs.

2.1.3 Section 3: Pricing

This section requests information regarding the pricing options and rates used by your company. Provide a description of your support services and available pricing options. Pricing options can include total price of an entirely new system and price leveraging SecureState’s existing system.

This section should include information on how you price engagements. For example, are they fixed bid, hourly rate, not to exceed, etc. The pricing options should include daily or hourly rates, expenses, and discounts. Please make sure your pricing details the cost for the system installation and the cost for annual monitoring and maintenance services.

3 Statement of Work

SecureState is requesting proposals from Security Integrators to enhance, upgrade, or replace the existing physical security system at its Cleveland headquarters.

3.1 Scope

Five major tasks have been identified for the System Integrator to perform as part of this project. The table below lists each of these tasks. These task are provided as guidance for how similar project have been completed. System Integrators are encouraged to outline in your response if additional tasks are needed or if tasks below need to be skipped or rearranged to achieve the goals of the project.

#	Task Name	Description
1	Card Readers	<ul style="list-style-type: none"> • Card readers with built-in keypads for SCIFs • Must integrate with existing iClass GR Cards • Minimum of 12 readers, two of which will require two-factor authentication



#	Task Name	Description
2	Cameras	<ul style="list-style-type: none">• Five new cameras inside the facility pointed at all badged doors• There are currently two external cameras, SecureState requires the two cameras to be moved for better coverage and one new external camera added.• Of the three total external cameras, two will need to be high resolution, with the capability to read license plates on vehicles entering or exiting the parking lot from the third floor. This may require the replacement of up to two existing cameras.• 30-day minimum data retention, with redundant drives
3	Alarm Systems	<ul style="list-style-type: none">• Alarm system must integrate badge readers, door contacts, cameras, and two-factor authentication systems• Auto-Alert sensors on doors• Must be able to track door/reader counts• Alarm system must include online management, with remote access through mobile devices and web (Mac friendly)<ul style="list-style-type: none">○ Must be able to set alarm remotely via mobile or web application○ Must be able to make adjustments to call list and users via app○ Must be able to view camera feeds remotely○ Web monitoring must account for dynamic IPs of SecureState users• Must have the ability to communicate over stable 4G connection or equivalent wireless protocol in the event of mainline failure
4	Service Level Agreements (SLAs)	<ul style="list-style-type: none">• Same-Day onsite service within eight hours for Medium priority service calls• Same-Day onsite service within two hours for High priority service calls
5	Service Appointments	<ul style="list-style-type: none">• Service Appointment scheduling processes must have transparent communication process with SecureState, including:<ul style="list-style-type: none">○ Email confirmation of ticket number and scheduled date and time○ Notification to SecureState if vendor support personnel will be early or late to service appointment○ Online option to confirm date/time or check appointment status