SCA

SECURITY COMPLIANCE ASSOCIATES

NETWORK PENETRATION TESTING
MSA ADDENDUM
FOR

Florida Housing

Finance Corporation

we make housing affordable

August 16, 2021

Table of Contents

Executive Summary

Florida Housing Finance Corporation (Florida Housing) was created by the state Legislature 35 years ago to assist in providing a range of affordable housing opportunities for residents that help make Florida communities great places in which to live, work and do business. Florida Housing's vision is to be recognized as an outstanding provider of innovative, measurable, data-driven and fiscally sustainable solutions that respond to the affordable housing challenges of our state.

Not unlike Florida Housing, Security Compliance Associates (SCA) is committed to providing superior services delivered in a manner to enhance loyalty. Our partner clients will testify on our abilities to perform top-notch assessment work, while respecting their individual culture. In advance, thank you for accepting this proposal and please know how important it is for us to assist you with any questions or clarifications.

SCA prides itself in identifying with our clients and working very closely to form a true partnership. We view this engagement as the beginning of a long-term relationship as your security partner, and not just a vendor. SCA will respond in a humanistic manner to all inquiries. Our practice includes the ability to use "plain English". With the deep experience of our associates, SCA is arguably the most seasoned provider for these services in the industry.

SCA follows client preferences for disseminating the results. Our philosophy includes openness. Individual assignments vary, however, please know that our experience includes interaction with all management, information technology, internal audit and committee members. SCA also welcomes board of director's interaction. Our reports are delivered in a manner that covers the entire scope of the engagement. They are segmented by the specific assessment phase in order to individually summarize and prioritize information on security risk, vulnerabilities, recommended countermeasures and corrective action.

Florida Housing seeks to test and validate network security through emulated Cyberattacks to replicate a threat actor who has gained access to the Florida Housing's virtual infrastructure as well as assess the integrity of existing firewall. Through SCA's remediation and corrective advice Florida Housing will be able to best position themselves to maintain best practices and industry standards moving forward.

To accomplish the above, SCA will provide very extensive Internal Network Penetration Testing and Firewall Assessment to allow Florida Housing to gain the best understanding of potential vulnerabilities, evaluate current controls to ensure information security and enhance the overall effectiveness of the cybersecurity and information protection program.

Company Overview

Security Compliance Associates, an Authorized HITRUST CSF® Assessor and GSA contract holder, was formed in June of 2005. SCA personnel have performed over 2,000 individual information security engagements nation-wide. These engagements include vulnerability assessments, penetration testing, application assessments, policy development, physical security, social engineering, information security training, controls review, NIST CSF assessments, risk assessments, HIPAA/HITECH Security Risk Analyses, HITRUST CSF Assessments and more.

SCA Project Staffing Team Leaders, who are introduced later in this proposal, and senior information security analysts are some of the best in the industry! Our analysts have been with us for 7 years on average and also have additional experience before joining SCA. Senior analysts who work with clients on-site have a CISSP (Certified Information Systems Security Professional) certification. Other certifications our analysts hold include:

- CCSFP – Certified CSF Practitioner
- CISA – Certified Information Systems Auditor
- C|EH – Certified Ethical Hacker
- OSCP - Offensive Security Certified Professional
- ITIL - Information Technology Infrastructure Library

Additionally, most of our senior analysts have earned a graduate degree in a related discipline including:

- Master of Science in Cybersecurity
- Master of Science in Digital Forensics
- Master of Science Information Technology
- Master of Science in Computer Information Systems

With more than 16 years of experience in delivering world class IT Information Security Assessment and Compliance services throughout the United States, our professionals bring over 200 years of combined Information Security experience, including time at NASA, the Department of Defense and the National Intelligence Community.

SCA is proud of our 'hands-on – relationship first' approach to providing our comprehensive suite of industry-leading security compliance services. We work in partnership with our clients' executive, information technology, risk management and audit functions in the process of delivering superior services and results. This close interaction ensures a high level of satisfaction and knowledge transfer throughout the engagement. Our reports are customized tailored for the audience and provide valuable, concise remediation advice, not just reams of data with no explanation. Helping our clients safeguard critical information, regardless of media, and complying with information security regulations, are the sole focus of SCA.

Security Compliance Associates is a GSA contract holder, number 47QTCA20D008C, to deliver Highly Adaptive Cybersecurity Services (HACS). Cage Code: 74NW7. DUNS 014545808.

GSA Contract Holder
47QTCA20D008C

SCA is active in and supports the following information security organizations:

(ISC)²® ISSA Information Systems Security Association International ISACA® INFRAGARD PARTNERSHIP FOR PROTECTION

Since we are privately held with no shareholders or private equity investors to satisfy, we can deliver world-class services for reasonable fees. In other words, SCA delivers big name/big 4 skill sets without the big cost.

Thank you for accepting this information! Florida Housing is a wonderful prospect, and we look forward to partnering with you, if we may.

Respectfully,

The SCA Team

Scope, Approach and Methodology

Per the spirit that defines advanced IT certifications such as CISSP, CISA, CCSFP, C|EH and OSCP, SCA is obligated to keep abreast of all new and anticipated threats to networks and environments, as well as current and evolving regulations. SCA utilizes a combination of commercially available tools, proprietary software and higher education to fulfill our responsibilities. Because of the diversity of our client base, SCA believes that we have a familiarity of systems, platforms and networks that will be hard to match, at any price.

SCA typically works directly with designated staff for preferences in delivering the services detailed in this proposal. Please refer to the service descriptions for additional details. We encourage Florida Housing personnel to actively participate in many of the assessment aspects, helping to share knowledge and understanding.

SCA follows a strict 4 stage process for all engagements, based upon NIST guidelines, that allows for a measurable, repeatable and defensible process as illustrated below:

PLANNING

During this phase, we will:

- Ensure all parties have a clear understanding of the scope and purpose of the engagement.
- Identify the assumptions and constraints associated with the project.
- Identify the personnel, controls and documentation that will be required for the engagement.
- Understand the model and analysis approach that will be used for the project.

DISCOVERY

Conduct onsite visits and interviews, gather and begin review of appropriate documentation, conduct assessment, compile data for analysis.

During this stage, we will:

- Identify threat sources and events
- Identify vulnerabilities and predisposing conditions
- Identify and communicate Critical Gap Findings (CGF)

REPORTING

During this stage, an analysis of all findings is conducted amongst our team to develop the draft report that determines:

- Likelihood of occurrence
- Magnitude of impact
- Risk to organization and maturity level of organization.

This allows us to develop the most appropriate strategies for remediation and plan for said remediation.

At the end of this stage, you will be presented with a Draft Report, and the executive summary of findings that will be used for the project.

COMMUNICATION

During this stage, we will:

- Deliver the final reports
- Present findings to management, committee and/or Board if requested.

External Services

Internal Network Penetration Testing and Firewall Assessment:

- SCA will conduct all requirements remotely via our External Services Team.

Florida Housing's and/or information security personnel are invited to "look over our shoulder" during the assessment. Details/targets of Florida Housing's environment for this engagement include (supplied by Florida Housing):

Main Location: 227 N. Bronough Street, Suite 5000 Tallahassee, Florida 32301

Internal IPs: 2 Class C Network (Active) - 7 Class C Network (total)

Servers: ~60 (>40 Virtual)

Workstations: ~150

Firewalls: 1 Redundant

Total Devices: ~350

Network Penetration Testing

Penetration testing subjects' systems to real-world attacks to gain system access or obtain sensitive information. Penetration Testing can be performed in one of three versions: White, Grey or Black Box. Each requires increasing amounts of Planning and Discovery effort to identify target assets.

Grey Box – partial knowledge of target systems and IP addresses in-scope

The phases of penetration testing include:

- Planning
- Discovery
- Attack - Exploitation
- Reporting
- Remediation Validation

Penetration testing frameworks and best practices used during engagements include the following:

Information	Description
Frameworks and Best Practices	• NIST SP 800-115 Technical Guide to Information Security Testing and Assessment • PTES - Penetration Testing Execution Standard • OSSTMM - Open Source Security Testing Methodology Manual • MITRE ATT&CK
Vulnerability Sources	• Carnegie Mellon's CERT.org (***www.cert.org***) • US Computer Emergency Readiness Team (***www.us-cert.gov***) • SANS Top 25 • OWASP Top 10 • Microsoft Security Advisories (***www.microsoft.com/security***)

Internal Penetration Testing

An Internal Penetration Test differs from a vulnerability assessment in that it exploits the vulnerabilities to determine what information is exposed. An Internal Penetration Test mimics the actions of an actual attacker or a rogue employee by exploiting weaknesses in network security without the usual dangers.

Planning

The first step of every penetration test begins with planning. During this phase, the rules of engagement are clearly identified and/or confirmed. These include the type of testing (white, grey or black box), testing goals and the client's preferences about notification and next steps when an exploitable vulnerability is found. Finally, management approval to begin testing is documented via a waiver and network information is shared as determined by the type of testing.

Discovery

Internal Penetration Testing Discovery includes Active Information Gathering:

Active Information Gathering
The Active Information Gathering Phase is where the internal systems for Florida Housing will be tested using various manual methods and automated tools which will form the foundation for the attack phase. During the active information gather phase, SCA will perform discovery and probing of targets in scope with the following technical activities:

- Port scanning
- OS fingerprinting
- Service enumeration
- Identifying misconfigurations
- Vulnerability analysis (manual testing and automated tools)
- Validation of discovered vulnerabilities

Attack - Exploitation

The Attack phase includes attempts to exploit found vulnerabilities to gain system access and/or sensitive information. Various techniques will be used including but not limited to manual techniques and automated tools. SCA will take precaution against disruption including a pre-assessment call in the Planning phase to clearly identify expectations, rules of engagement and the identification of systems to exclude from testing. During the pre-assessment call, the client also reserves the right to require approval of any attempted exploitation of systems/services prior to any attempts by SCA personnel. Any critical vulnerabilities are immediately brought to your attention, so they may be remediated.

Tools and resources used during the internal penetration test include, but are not limited to, the following:

NMAP	Hashcat
Metasploit Framework	Hydra
Nikto	Empire
Impacket Framework	BurpSuite
Exploit-db.com	Dirbuster
Sqlmap	WPScan
Hash Identifier	Theharvester
Responder	Mitm6
Mimikatz	Meterpreter
Securityfocus.com	SCA Developed Python Tools

Reporting

Upon completion, SCA will summarize the internal penetration testing results for each vulnerability with any information exploited, potential misconfigurations that could be leveraged and any remediation or mitigation techniques suggested. Information in this analysis includes:

- Open ports and service information
- Discovered vulnerabilities
- Methodologies used in identifying vulnerabilities
- Exploits attempted
- Exploits successfully executed
- Methodologies used in exploiting vulnerabilities
- Corrective/Remediation advice

Remediation Validation

Once remediation is complete, SCA will re-scan the target IP addresses in scope to validate remediation efforts. Since new vulnerabilities surface almost daily, it is possible that new vulnerabilities will be found with these scans. An agreed upon time allowance will be identified for remediation and should be reasonable in length to ensure timely project conclusion.

Firewall Assessment

During our Firewall Assessment, SCA will review boundary device configurations and architectures, perform vulnerability scans as needed and perform interviews with firewall/network administrators. Network diagrams and interviews with network administrators are conducted so that we can fully understand your network and its vulnerabilities.

During our Firewall Configuration Review, SCA will target high-level concepts by tracking specific points such as:

- Network diagrams and data flows
- Third party connections
- Filtering rules that blacklist or whitelist traffic
- Firewall rules management
- IDS / IPS location and alerting
- Process of monitoring alerts
- Access controls to administer devices
- Software updates
- Remediation recommendations

Deliverables

SCA provides custom reports for each project phase. The Internal Network Penetration Testing and Firewall Assessment reports are separate documents. The reports will reflect individual sections, highlighting each unique assessment focus and offer specific vulnerability findings, prioritization, recommendations and remediation advice. SCA allows for management comment columns, per request.

The reports are segmented and presented as follows:

- Table of Content
- Purpose
- Executive Summary-high level review of process and findings
- Vulnerability Classifications – identifies how each classification level, severe, high, medium, and low are defined.
- Approach and Methodology – explanation of various phases of the engagement.
- Assessment results- segmented by examined area
- Observations- with risk, background, and recommendations.
- Column for client response to findings

Draft reports are delivered in approximately 30 days from completion of testing. For larger engagements with multiple services and reports, please allow more time for delivery of draft reports. Florida Housing will have the opportunity to review the draft report with the SCA analyst and remediate findings within a reasonable amount of time before target assets are rescanned and the final report is delivered.

Project Management Approach

SCA has a history of working closely with clients. Assignments are much more fruitful when a relationship is developed from both standpoints. A typical assignment will begin with a conference call to introduce key personnel. Client preferences, expectations and timelines are identified. SCA intent is not to undermine your current efforts, but rather to work with you in an upfront manner to validate and document your posture. Interactive sessions will present alternatives to your practices and allow for consensus on remediation and course. Florida Housing will always be aware of pending report content, in advance, thus no surprises. SCA will honor Florida Housing preferences for each project phase.

Complementary Services

Security Compliance Associates delivers many more world-class information security and compliance services. Florida Housing may wish to consider the following either now or in the future:

- Information Security Risk Assessment
- NIST Cybersecurity Framework Assessment
- Controls Review (NIST 800-171, NIST 800-53, CIS CSC)
- Application Penetration Testing
- Information Security Policy and Procedures Program
- Disaster Recovery and Business Continuity Program
- Incident Response Program
- vCISO

Detailed and Annualized Fees

Florida Housing

Description	Annual	Unit	Total
	Qty.	Cost	
Internal Penetration Testing	1	$8,000	**$8,000**
(Grey Box, 500 active Ips)			
Firewall Assessment	1	$2,000	**$2,000**
(1 Redundant Firewall)			
Existing Client Discount			***($2,000)***
Total Annual Fees:			**$8,000**
Fees are valid for sixty (60) days from the date of this proposal			

Acceptance

The signatures below approve and accept this proposal as an addendum to the existing Master Services Agreement between Florida Housing Finance Corporation and Security Compliance Associates:

Security Compliance Associates:

By:____________________
(Authorized Signature)

Name: Brian Fischer

Title: Chief Revenue Officer

Date: 9/16/2021

Address:

2727 Ulmerton Rd., Suite 310
Clearwater, FL 33762

Telephone: 727-571-1141

Facsimile: 727-571-1140

Florida Housing Finance Corporation:

By:____________________
(Authorized Signature)

Name: Hugh R. Brown

Title: General Counsel

Date: 9-15-21

Address:

227 N. Bronough Street, Suite 5000
Tallahassee, FL 32301

Telephone: 850-448-4198

Facsimile: 850-488-9809

Project Team Staffing Leaders

SCA hiring policy prohibits the employment of convicted felons. No SCA employee has been convicted of a felony. SCA employee eligibility to work in the United States is confirmed through e-Verify upon hire. SCA carries multi-million-dollar errors and omissions coverage. The table below lists team members who will be assigned to this project based upon availability and need. We have provided a brief summary of each resource's skill sets and how they are relevant to the scope of work detailed in this proposal. Based on availability, and upon the contract award, more comprehensive candidate resumes can be furnished upon request.

POSITION	CANDIDATE SUMMARY	CREDENTIALS
CIO	**Jim Catrett MSIT** began with SCA as an Information Security Compliance Senior Analyst with an educational background focused on Information Assurance and Security. Jim ascended to VP of Compliance Services where he managed SCA'a compliance portfolio of services, Now as CIO, Jim is responsible for the delivery of SCA's entire portfolio of services. Jim has performed over 150 information security risk assessments and policy/procedure review and development programs. Jim is driven to assist organizations in exceeding compliance and regulatory requirements regarding information security. He received a Master of Science in Information Technology focusing on Information Assurance and Security with a concentration on Policy and Procedures and Business Continuity Development.	MSIT, CCSFP
CISO	**Maja Bobic, CISSP, CISA, CCSFP**, is an information security professional with a Bachelor degree in MIS with a concentration in Information Security from Florida Atlantic University. Maja has managed and performed vulnerability assessments and penetration tests for multi-million and multi-billion dollar asset financial institutions providing vital information on vulnerabilities and solutions to ensure the integrity and security of client networks. Maja's extensive information security experience includes Network Security, Risk Assessments and Audit Program Compliance, Information Security Standards and Best Practices, Security Monitoring and Risk Mitigation, Vulnerability Assessments and Penetration Testing and Information Security Policy Review and Development. She provides solutions for effective incident response to clients in order to minimize impact on daily operations and conducts information security analysis using NIST SP 800-53 revision 4, ISO 27001 and others. Maja also executes physical security assessments, performs social engineering exercises and has reviewed client network architecture and design and recommended changes for network security improvement. Maja leverages her impressive grasp of cyber security best practices and analytical capabilities to meet our clients specific needs.	CISSP CISA CCSFP, CHQP

POSITION	CANDIDATE SUMMARY	CREDENTIALS
VP of Cybersecurity Services	**Jacob Wattam, CE|H, OSCP,** holds a Master of Science in Cyber Security and Digital Forensics from the University of South Florida. Jacob's background is diverse - ranging from systems administration and network security to managing a team of more than fifty staff members for a Fortune 500 company. Jacob has in-depth knowledge of penetration testing techniques, vulnerability analysis and network forensics, as well as commercial, open-source and custom information security and forensics tools. Jacob manages SCA's deep dive penetration testing, focusing on clients that have mature information security programs and history. Jacob is an expert in evaluating electronic commerce web applications, providing clients a comfort level that their internet facing applications are configured securely and deployed properly. Jacob's efforts have allowed SCA to become an acknowledged and preeminent provider for these services.	M.S. Cybersecurity/ Digital Forensics C|EH OSCP