



BULLETPROOF

a GLI company

Bulletproof Solutions, Inc.

7160 Amigo Street
Las Vegas, Nevada
USA | 89119

Tel: 1-866-328-5538

Web: www.bulletproofsi.com

**Response to
Invitation for Bid
IFB # 710-20-0005
Security and Privacy Control
Assessment (SCA)**

**Prepared for
State of Arkansas
Department of Human Services**

BID RESPONSE PACKET

Submission Date:
November 22, 2019 by 2:00PM CDT

Table of Contents

Executive Summary..... 1
Bid Signature Page..... 2
Section 1 – Vendor Agreement and Compliance..... 3
Section 2 – Vendor Agreement and Compliance..... 4
Section 3 – Vendor Agreement and Compliance..... 5
Section 4 – Vendor Agreement and Compliance..... 6
Proposed Subcontractors Form 7
Attachment A – EO 98-04 Disclosure Form..... 8
Equal Opportunity Policy..... 9
Addenda Acknowledgement..... 10
Minimum Qualifications..... 11
 Letter of Bondability..... 11
 Financial Statement..... 12
 Qualifications and Experience 13
Appendix 1 – Resumes..... 19

Executive Summary

The State of Arkansas Department of Human Services (DHS) seeks the services of a qualified firm to perform Security and Privacy Control Assessment (SCA) services in support of the deployment of the new Integrated Eligibility and Benefit Management Solution.

Bulletproof Solutions, Inc. (Bulletproof) will partner with its affiliated company, SeNet International Corporation (SeNet) to provide SCA services for the DHS. Both companies are part of the Gaming Laboratories International (GLI) group of companies. GLI has been providing security services since 2011. Over the past several years, GLI expanded with the addition of like-minded companies dedicated to delivering compliance assurance and risk mitigating services with the same vision, drive and innovation. The GLI group of companies includes Bulletproof, acquired in 2016 and SeNet which was acquired earlier this year.

This partnership between Bulletproof and SeNet provides the DHS with a deep level of security expertise that makes our team the clear choice for this project. Bulletproof was founded in 2000 and began operations in 2001 as a Security Consulting Firm. For the past 18 years, Bulletproof has been providing information technology (IT) security expertise to equip our clients with solutions that help them mitigate risk, achieve compliance, and protect their businesses. SeNet is an IT cybersecurity consulting firm that has been providing expert-level information security consulting services to public and private sector clients including many U.S. government entities for more than 21 years. SeNet is an innovative leader in IT services, specializing in networking and information systems security.

Bulletproof and SeNet working together provide world renowned experience, innovative security solutions, and a relationship and resources you can trust

Our proposed team has the experience and skills to perform the range of security tasks that the DHS requires including prior experience conducting similar services for U.S state governments.

Together, these two companies provide unmatched value for our clients: world renowned experience, innovative security solutions, and a relationship and resources you can trust. Our unique combination of expertise provides a razor-sharp focus on protecting your assets in today's evolving IT and security landscape. As the threat and control landscape continues to evolve—exponentially—you can be assured that you have access to world-class expertise.

Bid Signature Page

BID SIGNATURE PAGE

Type or Print the following information.

PROSPECTIVE CONTRACTOR'S INFORMATION				
Company:	Bulletproof Solutions, Inc.			
Address:	7160 Amigo Street			
City:	Las Vegas	State:	NV	Zip Code: 89119
Business Designation:	<input type="checkbox"/> Individual <input type="checkbox"/> Sole Proprietorship <input type="checkbox"/> Public Service Corp <input type="checkbox"/> Partnership <input checked="" type="checkbox"/> Corporation <input type="checkbox"/> Nonprofit			
Minority and Women-Owned Designation*:	<input type="checkbox"/> Not Applicable <input type="checkbox"/> American Indian <input type="checkbox"/> Asian American <input type="checkbox"/> Service Disabled Veteran <input type="checkbox"/> African American <input type="checkbox"/> Hispanic American <input type="checkbox"/> Pacific Islander American <input type="checkbox"/> Women-Owned			
	AR Certification #: _____		* See <i>Minority and Women-Owned Business Policy</i>	

PROSPECTIVE CONTRACTOR CONTACT INFORMATION			
Provide contact information to be used for bid solicitation related matters.			
Contact Person:	Gus Fritschie	Title:	VP, IT Security Solutions Development & Delivery USA
Phone:	301-215-7684	Alternate Phone:	
Email:	procurement@bulletproofsi.com		

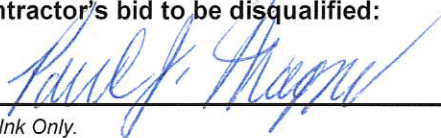
CONFIRMATION OF REDACTED COPY
<input checked="" type="checkbox"/> YES, a redacted copy of submission documents is enclosed. <input type="checkbox"/> NO, a redacted copy of submission documents is <u>not</u> enclosed. I understand a full copy of non-redacted submission documents will be released if requested.
<i>Note: If a redacted copy of the submission documents is not provided with Prospective Contractor's response packet, and neither box is checked, a copy of the non-redacted documents, with the exception of financial data (other than pricing), will be released in response to any request made under the Arkansas Freedom of Information Act (FOIA). See Bid Solicitation for additional information.</i>

ILLEGAL IMMIGRANT CONFIRMATION
By signing and submitting a response to this <i>Bid Solicitation</i> , a Prospective Contractor agrees and certifies that they do not employ or contract with illegal immigrants. If selected, the Prospective Contractor certifies that they will not employ or contract with illegal immigrants during the aggregate term of a contract.

ISRAEL BOYCOTT RESTRICTION CONFIRMATION
By checking the box below, a Prospective Contractor agrees and certifies that they do not boycott Israel, and if selected, will not boycott Israel during the aggregate term of the contract. <input checked="" type="checkbox"/> Prospective Contractor does not and will not boycott Israel.

An official authorized to bind the Prospective Contractor to a resultant contract must sign below.

The signature below signifies agreement that any exception that conflicts with a Requirement of this *Bid Solicitation* will cause the Prospective Contractor's bid to be disqualified:

Authorized Signature:  Title: Executive Vice President
Use Ink Only.

Printed/Typed Name: Paul J. Magno Date: November 20, 2019

Section 1 – Vendor Agreement and Compliance

SECTION 1 - VENDOR AGREEMENT AND COMPLIANCE

- Any requested exceptions to items in this section which are NON-mandatory **must** be declared below or as an attachment to this page. Vendor **must** clearly explain the requested exception, and should label the request to reference the specific solicitation item number to which the exception applies.
- Exceptions to Requirements **shall** cause the vendor's proposal to be disqualified.

By signature below, vendor agrees to and **shall** fully comply with all Requirements as shown in this section of the bid solicitation.

Vendor Name:	Bulletproof Solutions, Inc.	Date:	November 20, 2019
Signature:		Title:	Executive Vice President
Printed Name:	Paul J. Magno		

Section 2 – Vendor Agreement and Compliance

SECTION 2 - VENDOR AGREEMENT AND COMPLIANCE

- Any requested exceptions to items in this section which are NON-mandatory **must** be declared below or as an attachment to this page. Vendor **must** clearly explain the requested exception, and should label the request to reference the specific solicitation item number to which the exception applies.
- Exceptions to Requirements **shall** cause the vendor's proposal to be disqualified.

By signature below, vendor agrees to and **shall** fully comply with all Requirements as shown in this section of the bid solicitation.

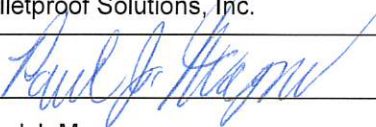
Vendor Name:	Bulletproof Solutions, Inc.	Date:	November 20, 2019
Signature:		Title:	Executive Vice President
Printed Name:	Paul J. Magno		

Section 3 – Vendor Agreement and Compliance

SECTION 3 - VENDOR AGREEMENT AND COMPLIANCE

- *Exceptions to Requirements shall cause the vendor's proposal to be disqualified.*

By signature below, vendor agrees to and **shall** fully comply with all Requirements as shown in this section of the bid solicitation.

Vendor Name:	Bulletproof Solutions, Inc.	Date:	November 20, 2019
Signature:		Title:	Executive Vice President
Printed Name:	Paul J. Magno		

Section 4 – Vendor Agreement and Compliance

SECTION 4 - VENDOR AGREEMENT AND COMPLIANCE

- *Exceptions to Requirements shall cause the vendor's proposal to be disqualified.*

By signature below, vendor agrees to and **shall** fully comply with all Requirements as shown in this section of the bid solicitation.

Vendor Name:	Bulletproof Solutions, Inc.	Date:	November 20, 2019
Signature:		Title:	Executive Vice President
Printed Name:	Paul J. Magno		

Proposed Subcontractors Form

PROPOSED SUBCONTRACTORS FORM

- **Do not** include additional information relating to subcontractors on this form or as an attachment to this form.

PROSPECTIVE CONTRACTOR PROPOSES TO USE THE FOLLOWING SUBCONTRACTOR(S) TO PROVIDE SERVICES.

Type or Print the following information

Subcontractor's Company Name	Street Address	City, State, ZIP
SeNet International Corporation	3040 Williams Drive, Suite 510	Fairfax, VA 22031

PROSPECTIVE CONTRACTOR DOES NOT PROPOSE TO USE SUBCONTRACTORSTO PERFORM SERVICES.

By signature below, vendor agrees to and **shall** fully comply with all Requirements related to subcontractors as shown in the bid solicitation.

Vendor Name:	Bulletproof Solutions, Inc.	Date:	November 20, 2019
Signature:		Title:	Executive Vice President
Printed Name:	Paul J. Magno		

Attachment A – EO 98-04 Disclosure Form

CONTRACT AND GRANT DISCLOSURE AND CERTIFICATION FORM

Failure to complete all of the following information may result in a delay in obtaining a contract, lease, purchase agreement, or grant award with any Arkansas State Agency.

SUBCONTRACTOR: _____ SUBCONTRACTOR NAME: _____
 Yes No

IS THIS FOR: **Goods? Services? Both?**

TAXPAYER ID NAME: _____

YOUR LAST NAME: _____ FIRST NAME _____ M.I.: _____

ADDRESS: _____

CITY: _____ STATE: _____ ZIP CODE: _____ COUNTRY: _____

AS A CONDITION OF OBTAINING, EXTENDING, AMENDING, OR RENEWING A CONTRACT, LEASE, PURCHASE AGREEMENT, OR GRANT AWARD WITH ANY ARKANSAS STATE AGENCY, THE FOLLOWING INFORMATION MUST BE DISCLOSED:

FOR INDIVIDUALS *

Indicate below if: you, your spouse or the brother, sister, parent, or child of you or your spouse is a current or former: member of the General Assembly, Constitutional Officer, State Board or Commission Member, or State Employee:

Position Held	Mark (√)		Name of Position of Job Held [senator, representative, name of board/ commission, data entry, etc.]	For How Long?		What is the person(s) name and how are they related to you? [i.e., Jane Q. Public, spouse, John Q. Public, Jr., child, etc.]	
	Current	Former		From MM/YY	To MM/YY	Person's Name(s)	Relation
General Assembly							
Constitutional Officer							
State Board or Commission Member							
State Employee							

None of the above applies

FOR AN ENTITY (BUSINESS) *

Indicate below if any of the following persons, current or former, hold any position of control or hold any ownership interest of 10% or greater in the entity: member of the General Assembly, Constitutional Officer, State Board or Commission Member, State Employee, or the spouse, brother, sister, parent, or child of a member of the General Assembly, Constitutional Officer, State Board or Commission Member, or State Employee. Position of control means the power to direct the purchasing policies or influence the management of the entity.

Position Held	Mark (√)		Name of Position of Job Held [senator, representative, name of board/commission, data entry, etc.]	For How Long?		What is the person(s) name and what is his/her % of ownership interest and/or what is his/her position of control?		
	Current	Former		From MM/YY	To MM/YY	Person's Name(s)	Ownership Interest (%)	Position of Control
General Assembly								
Constitutional Officer								
State Board or Commission Member								
State Employee								

None of the above applies

Contract Number 710-20-0005
Attachment Number A
Action Number _____

Contract and Grant Disclosure and Certification Form


Failure to make any disclosure required by Governor's Executive Order 98-04, or any violation of any rule, regulation, or policy adopted pursuant to that Order, shall be a material breach of the terms of this contract. Any contractor, whether an individual or entity, who fails to make the required disclosure or who violates any rule, regulation, or policy shall be subject to all legal remedies available to the agency.

As an additional condition of obtaining, extending, amending, or renewing a contract with a state agency I agree as follows:

1. Prior to entering into any agreement with any subcontractor, prior or subsequent to the contract date, I will require the subcontractor to complete a **CONTRACT AND GRANT DISCLOSURE AND CERTIFICATION FORM**. Subcontractor shall mean any person or entity with whom I enter an agreement whereby I assign or otherwise delegate to the person or entity, for consideration, all, or any part, of the performance required of me under the terms of my contract with the state agency.
2. I will include the following language as a part of any agreement with a subcontractor:

Failure to make any disclosure required by Governor's Executive Order 98-04, or any violation of any rule, regulation, or policy adopted pursuant to that Order, shall be a material breach of the terms of this subcontract. The party who fails to make the required disclosure or who violates any rule, regulation, or policy shall be subject to all legal remedies available to the contractor.
3. No later than ten (10) days after entering into any agreement with a subcontractor, whether prior or subsequent to the contract date, I will mail a copy of the **CONTRACT AND GRANT DISCLOSURE AND CERTIFICATION FORM** completed by the subcontractor and a statement containing the dollar amount of the subcontract to the state agency.

I certify under penalty of perjury, to the best of my knowledge and belief, all of the above information is true and correct and that I agree to the subcontractor disclosure conditions stated herein.

Signature  Title Paul J. Magno, Executive Vice President Date November 20, 2019
Vendor Contact Person Gus Fritschie Title VP, IT Security Solutions Development & Deployment Phone No. (301) 215-7684

Agency use only

Agency Number 0710 Agency Name Department of Human Services Agency Contact Person _____ Contact Phone No. _____ Contract or Grant No. _____

Equal Opportunity Policy

As per Bulletproof's Employee Handbook, the following is the company's Equal Opportunity Policy:

Bulletproof Solutions Employee Handbook

**EQUAL EMPLOYMENT OPPORTUNITY, SEXUAL HARASSMENT
AND ANTI-BULLYING**

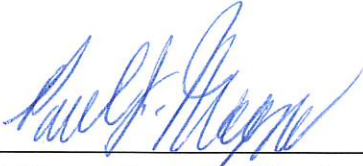
6.0 EQUAL EMPLOYMENT OPPORTUNITY

Bulletproof Solutions is committed to equal opportunity employment. Bulletproof Solutions is committed to employing all persons who qualify based on merit and ability alone.

Implementation of this requirement by Bulletproof Solutions Management and all employees ensures a safe, healthy and productive work environment and assures compliance with legal requirements.

Addenda Acknowledgement

Bulletproof Solutions, Inc. acknowledges that this IFB was amended on November 7, 2019.



Paul J. Magno, Executive Vice President

November 20, 2019

Date

Minimum Qualifications

Letter of Bondability

The Contractor must meet the following requirements:

A. The Vendor must be bondable. As proof of meeting this qualification the Vendor must include a letter of bondability.

Financial Statement

B. The Vendor (Prime) must have annual revenue of at least five million dollars (\$5M). As proof of meeting this qualification; the Vendor must include a copy of their most recent independent audited financial statement or tax return.

Evidence of our financial statements are provided in a separate sealed envelope.

Qualifications and Experience

References

C. The Vendor's team (Prime and/or Subcontractor) must be able to perform SCA services in support of the development of State IT systems that determine eligibility for the Medicaid program. For verification purpose, Vendor shall provide the following:

1. At least two (2) past performance examples of similar function services performed in other states within the past five (5) years. Services performed can include both contract and direct employment. For each referenced project, the vendor shall provide
 - a. A description of the work performed;
 - b. The time period and project amount;

Since each task has both common as well as unique requirements, Bulletproof proposes a project team with a mix of skill sets that cover the scope and size required for the specific effort. A complex project such as the SCA requested by the DHS calls for technical and analytical expertise.

Our team is more than qualified to perform SCA services in support of the development of State IT systems that determine eligibility for the Medicaid program. Bulletproof and its staff have earned multiple awards and certifications for technical competence and outstanding performance. Our awards are a credit to our staff's perseverance and ability to get the job done right the first time.

Bulletproof has developed extensive expertise in conducting comprehensive security compliance reviews and analyses for multiple commercial and government clients. Over the years, our IT security specialists perfected the process, the methodology, the tools, and the documentation that are required to perform the tasks of the scope and complexity similar to that of the DHS.

The following are a few of the projects the proposed team members have completed that relate to this opportunity:

Customer Name and Address:	
Point of Contact Name, Phone, and Email:	
Contract Title:	
Period of Performance:	
Total Contract Value:	
Relevancy of Project to SOW:	
<p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>	
Schedule or Quality Concerns?	Problems, Delays, Cost Overruns, and/or any Corrective Actions Taken?
[REDACTED]	[REDACTED]
Performance Assessment:	
[REDACTED]	

Customer Name and Address:	
Point of Contact Name, Phone and Email:	
Contract Title:	
Period of Performance:	
Total Contract Value:	
Relevancy of Project to SOW:	
Scope of Project	
<ul style="list-style-type: none"> █ [Redacted] █ [Redacted] █ [Redacted] █ [Redacted] █ [Redacted] █ [Redacted] █ [Redacted] 	
Schedule or Quality Concerns?	Problems, Delays, Cost Overruns and/or any Corrective Actions Taken?
█	█
Performance Assessment:	
█	

Customer Name and Address:	
Point of Contact Name, Phone, and Email:	
Contract Title:	
Period of Performance:	
Total Contract Value:	
Relevancy of Project to SOW:	
Scope of Project	
<ul style="list-style-type: none"> █ [REDACTED] █ [REDACTED] 	
<ul style="list-style-type: none"> █ [REDACTED] 	
<ul style="list-style-type: none"> █ [REDACTED] 	
Schedule or Quality Concerns?	Problems, Delays, Cost Overruns, and/or any Corrective Actions Taken?
█	█
Performance Assessment:	
█	

Projected Key Staff and Work History Resumes

Work history resumes for vendor's key staff, which shall include relevant projects (past and current) that each individual has supported for a state Medicaid program.

The work history resume submitted for the proposed key individuals on this project must show past SCA work on at least one (1) eligibility engagement that supported a state Medicaid system.

Primary Contact

Mr. Gus Fritschie, Bulletproof's Vice President, IT Security Solutions Development & Delivery USA will be your primary contact serving as account manager and technical contact. Mr. Fritschie has led and performed numerous vulnerability assessments and penetration tests in support of financial audits and other compliance-related efforts. Clients included Fortune 500 companies, civilian agencies, and the Department of Defense (DOD). Mr. Fritschie has led several large-scale projects. Some projects included enterprise-wide vulnerability assessments for multiple government and commercial clients, management of Certification and Accreditation (C&A) efforts, and web application penetration tests.

Mr. Fritschie has proven work performance with organizations and clients such as the Department of Health and Human Services (HHS), the Department of Agriculture (USDA), the Department of Labor (DOL), the Department of the Interior (DOI), the Government Printing Office (GPO), and Amtrak.

Project Manager and Staff

The Lead Assessor assigned to this project will be our Senior Security Analyst, Mr. Phillip Young. Mr. Young has served as Team Lead/Project Manager and the Senior Security Analyst for several large-scale projects, including a multi-year project with the Department of Education (ED) Office of the Inspector General (OIG). As it relates to this project, Mr. Young has led both projects with the State of Nevada (SSHIX and DHHS) as well as the Minnesota MNSure project. He is also an accomplished IT Auditor, experienced in performing Federal Information Security Modernization Act (FISMA) reviews. In addition to Mr. Fritschie and Mr. Young, our team is comprised of the following team members:

- **Mr. Roey Katz, CISSP, Sr. Security Analyst**—Mr. Katz is seasoned in application security, experienced in developing and implementing secure systems and solutions, and knowledgeable in computer networks and programming. He is the lead developer for the OWASP ByWAF project and is proficient in many languages including Python, .NET, and Java. He possesses a strong academic background with heavy emphasis on computer architecture and network security. He possesses expert-level knowledge in Linux. A BSCE, Mr. Katz has his Master's degree in Information Security Engineering from Johns Hopkins University in Baltimore, Maryland.

- Mr. Elijah Matthews, Cybersecurity Analyst**—Mr. Matthews is a Cybersecurity Analyst with experience in updating information Security System Policies and establishing baselines in accordance with NIST, FISMA, and other industry best practices. He has experience in performing vulnerability assessments to detect potential risks in single or multiple assets across an enterprise network. Mr. Matthews is also experienced in performing updates of IT security policies, procedures, standards, and guidelines per Federal requirements.

Table 1 provides a list of proposed personnel. The information provided in this table is intended to demonstrate in a concise format the depth of the length, variety, and relevant experience and expertise our highly experienced staff brings to this project on day one.

Table 1: Proposed Personnel

Name	Proposed Position	Education	Certifications	Experience	Skills
Phillip Young, Jr.	Lead Assessor/Project Manager	B.S., Accounting	CISA (pending)	Sr. IT Analyst/Team Lead (2012–Present) IT Supervisor/Project Manager (2008–2012) Sr. IT Auditor (2007–2008) Sr. Accountant/Auditor (2003–2007) Staff Accountant (2001–2003)	Team Lead IT Security Audit Security Assessment FISMA Audit
Roey Katz	Sr. Security Analyst	M.S., Information Security B.S., Computer Engineering	CISSP	Sr. Security Engineer (2003–Present)	Application Security Database Assessments FISMA/PCI Compliance Security Reviews
Elijah Matthews	Cybersecurity Analyst	M.S., Information Systems B.S., Computer Science	CompTIA Security + CAP (pending)	Cybersecurity Analyst (2019–Present) Cybersecurity Jr. Analyst (2018–2019) IT Support Specialist (2017–Present) Information Assurance Analyst (2016–2018)	Cybersecurity Analyst Security Reviews Penetration Testing Vulnerability Assessment

Full resumes for our proposed team are provided in **Appendix 1 – Resumes**.

Appendix 1 – Resumes

Phillip Young, Jr.

Project Manager



(703) 206-9383



Phillip.Young@senet-int.com



Fairfax, VA

EDUCATION

B.S., Accounting, Hampton University
Hampton, VA

Certifications

Certified Information Systems
Auditor (CISA) Candidate

PROFESSIONAL PROFILE

Mr. Young is a seasoned Information Technology (IT) Auditor, experienced in performing Federal Information Security Modernization Act (FISMA) reviews on the Department of Education's (ED) Office of Inspector General (OIG) Information Technology Audits Division.

SCA WORK EXPERIENCE

SeNet International Corporation | Fairfax, VA | 2012 – Present

Mr. Young has been a SeNet employee for 7 years.

Position on following SCA Projects: Project Manager/Team Lead
Years of SCA experience: 7

Minnesota Marketplace Exchange (MNSure) (9/2019-11/2019)

Oversaw the security assessment task issued by GetInsured for the Minnesota Marketplace Exchange (MNSure) in which SeNet performed a security and privacy controls assessment. This contract includes performing a security assessment of the full control suite in the System Security Plan (SSP) for the MNSure web application in accordance with the Centers for Medicare and Medicaid Services (CMS) Minimum Acceptable Risk Standards for Exchanges (MARS-E 2.0) Security Assessment Control

POC: Deb Schierbaum, Manager, Data Operations and InfoSec; Phone: (253) 209-0082

State of Nevada Silver State Health Insurance Exchange (SSHIX) (2/019-6/2019)

Conducted a MARS-E v2.0 Independent Security Assessment. The purpose of this Security Controls Assessment (SCA) was to determine whether the security and privacy controls were implemented correctly, operated as intended, and produced the desired outcomes for meeting the security and privacy requirements of the information system. The assessment reflected the security and privacy posture at the time of the SCA while other MARS-E controls address ongoing monitoring of control implementation.

- Supplied a MARS-E v2.0 Security Assessment Report (SAR) per the guidance outlined within the CMS Framework for the Independent Assessment of Security and Privacy Controls
- The SAR appropriately assessed all security and privacy controls defined in the CMS MARS-E Control Framework
- Documented all recommendations within the current CMS Plan of Actions and Milestones (POA&M) template for SSHIX

POC: Eric Watt: Sr. Project Manager; Phone: (971) 261-7777 SeNet completed the following tasks:

Ceannate Corporation: (2017, 2018, 2019)

Conducted an audit that assessed the full control suite in the System Security Plan (SSP) for Corporation applications in accordance with NIST 800-53, Revision 4 Security Controls, including production of the Security Assessment Report (SAR).

POC: David Bradley, Director of Information Security; Phone: (888) 853-8148, ext. 4170

Phillip Young, Jr.

Clearances

Public Trust

EXPERIENCE *CONTINUED*

For the North Carolina Education Lottery (NCEL) (2015 and 2017)

Conducted an audit that:

- Assessed whether effective IT security controls were in place and being followed;
- Evaluated controls in place to protect the confidentiality, integrity and availability of the client's systems and data; and
- Identified potential security risks and analyzed possible opportunities for improvements.

POC: Noboru "Tony" Chung, DED of MIS/GS; Phone: (919) 301-3501

For the Florida Lottery (2016 and 2018)

Conducted an audit that:

- Assessed whether effective IT security controls were in place and being followed;
- Evaluated controls in place to protect the confidentiality, integrity and availability of the client's systems and data; and
- Identified potential security risks and analyzed possible opportunities for improvements.

POC: Jack May, Deputy Director Information Security Management; Phone: (850) 487-7777, ext. 2178

Government Printing Office (GPO) (Present)

- Evaluated controls in place to protect the confidentiality, integrity, and availability of the GPO systems
- Updated the System Security Plans (SSP) and System Characterization Documents (SCD) in accordance with NIST, FISMA, FIPS, GAGAS and industry best security practices

POC: John Hannan, Director IT Security; Phone: (202) 512-1021

Skills

- **Desktop Applications:** Microsoft Office: Excel, Access, Word, PowerPoint; VMWare; TeamMate; IDEA Data Analysis Software; CoreImpact Professional

Roey Katz, CISSP

S e n i o r S e c u r i t y A n a l y s t



(703) 206-9383



Roey.Katz@senet-int.com



Fairfax, VA

EDUCATION

M.S., Information Security,
Johns Hopkins University

B.S., Computer Engineering
University of Maryland

Certifications

Certified Information Systems
Security Professional (CISSP)

PROFESSIONAL PROFILE

Mr. Katz is seasoned in Certification and Accreditation (C&A), experienced in developing and implementing secure systems and solutions, and knowledgeable in computer networks and programming. He possesses a strong academic background with a heavy emphasis on computer architecture and network security. He possesses expert-level knowledge in Linux.

SCA WORK EXPERIENCE

SeNet International Corporation | Fairfax, VA | 2003 – Present

Mr. Katz has been an employee of SeNet for 16 years.

Position on following SCA projects: Sr. Security Analyst

Years of SCA experience: 16 years

- **Commonwealth of Kentucky CHFS (2017):** Led NIST 800-53 Interviews and Examinations (I&E) sessions for ATO.
POC: Bryan Lykins, CISA, CFE (Manager of Audits and Compliance); Phone: (502) 564-0105 ext. 2927
- **Virginia Lottery (2/2017-4/2017):** Led NIST 800-53 and Multi-State Lottery Association (MUSL) Interviews and Examinations (I&E) sessions for ATO.
POC: Joe Hubbell, Information Security; Phone:
- **South Carolina Housing (2016, 2017, 2018, and 2019):** Led NIST 800-53 and FedRAMP Interviews and Examinations (I&E) sessions for ATO; performed technical assessment with penetration testing.
POC: Del Collins, IT Director; Phone: (803) 896-9001
- **North Carolina FAST (2017):** Led NIST 800-53 Interviews and Examinations (I&E) sessions for ATO.
POC: Charles Carter, Information Security Specialist; Phone: (919) 855-3000
- **Idaho Department of Health and Welfare (11/2014-2/2015 and 4/2019-6/2019):** Led NIST 800-53 Interviews and Examinations (I&E) sessions for ATO.
POC: Scott Knights, Senior Agency Information Security Officer; Phone: (208) 334-6547
- **Dept. of Education Office of the Inspector General (8/2014-2018):** Led NIST 800-53 Interviews and Examinations (I&E) sessions for ATO; performed technical assessment with penetration testing.
POC: Therese Campbell, Assistant Director IT Audit Division/COR; Phone: (202) 245-7367

State of Nevada Silver State Health Insurance Exchange (SSHIX) (2/019-6/2019)

Conducted a MARS-E v2.0 Independent Security Assessment. The purpose of this Security Controls Assessment (SCA) was to determine whether the security and privacy controls were implemented correctly, operated as intended, and produced the desired outcomes for meeting the security and privacy requirements of the information system.

POC: Eric Watt, Sr. Project Manager; Phone: (971) 261-7777

SeNet completed the following tasks:

- Supplied a MARS-E v2.0 Security Assessment Report (SAR) per the guidance outlined within the CMS Framework for the Independent Assessment of Security and Privacy Controls
- The SAR appropriately assessed all security and privacy controls defined in the CMS MARS-E Control Framework
- Documented all recommendations within the current CMS Plan of Actions and Milestones (POA&M) template for SSHIX

Roey Katz

Clearances

OPM Public Trust

SCA EXPERIENCE *CONTINUED*

United States Department of Agriculture (USDA) (11/2009-3/2013), Mr. Katz has provided security testing expertise to the USDA to support the C&A process for several USDA components, including the NFC, Departmental Administration (DA), and Office of the Chief Information Officer (OCIO)

POC: Rick Culotta, IT Security; Phone: (504) 426-1047

- Mr. Katz performed testing and was responsible for the results documented in the Security Assessment Report (SAR). He also performed risk assessments and created and assisted in Plan of Actions and Milestones (POA&M) development. The C&A documentation followed USDA templates and standards.

Health and Human Services (HHS) Health Resources and Services Administration (HRSA) (11/2007-8/2014): as part of an on-site team assisting the Office of the Chief Information Security Officer, Mr. Katz:

POC: Richard Woodruff (retired); Email: Richard.woodruff@hotmail.com

- Drafted and reviewed security policies and procedures for HRSA's information technology network.
- Compiled a full inventory of HRSA's network components.
- Evaluated HRSA's desktops against the Federal Desktop Core Configuration (FDCC) initiative.
- Explored and tested network security monitoring tools such as Secure Fusion.
- Performed security monitoring in HRSA's security operations center (SOC) utilizing tools such as Snort and NetIQ Security Manager.

For SeNet clients, Mr. Katz (2003-Present):

- Has performed NIST 800-series C&A efforts for several agencies in the areas of risk management, contingency planning, incident response, disaster recovery, and vulnerability assessment.
- Drafts policies for department-wide security programs covering the entire range of National Institute of Standards and Technology (NIST) 800-53 control families.
- Develops procedures, DISA Security Technical Implementation Guides (STIGs), and other baselines for management and administration of heterogeneous networks of hardware and software (Juniper, Cisco, Oracle, Sun and Linux) for both Federal and commercial clients.
- Explores upcoming trends in security technologies, including intrusion detection systems (IDSs), virtual private networks (VPNs), firewalls, and Windows and UNIX system security.

Skills

- **Security Tools:** Nessus, Nmap, Burp, Zap, AppScan, AppDetective, Netsparker, Core Impact, Nikto, Microsoft Baseline Security Analyzer (MBSA), Superscan, NGS-Squirrel, Defense Information Systems Agency (DISA) Gold Disc, Nessus Compliance Tool, in-house developed tools
- **Firewalls and VPNs:** Check Point VPN-1, SecuRemote, Panda Antivirus, Trend Micro Antivirus, NetScreen NS-25, NetScreen-Remote, OpenVPN, NetIQ, Snort
- **Backup and Antivirus:** Veritas BackupExec and Symantec, Panda and Trend Micro Antivirus
- **Communications:** Exchange, Postfix, Postgrey, Bind DNS, OpenSSL, Apache, Active Directory
- **Operating Systems:** Microsoft Windows 2010, Ubuntu, Debian, and Red Hat GNU/Linux
- **Languages:** C, C++, Java, Linux, Perl, Python
- **Desktop Applications:** Microsoft Office Suite – Word, Excel, PowerPoint, Visio, and Outlook

Elijah Matthews

C y b e r s e c u r i t y A n a l y s t



(703) 206-9383



Elijah.Matthews@senet-int.com



Fairfax, VA

EDUCATION

M.S. Information Systems, George Washington University (2020)

B.S., Computer Science, Simon Fraser University, 2014

United States Army Cyber Center of Excellence 2017

Certifications

CompTIA Security +

CAP Certification (in progress)

PROFESSIONAL PROFILE

Mr. Matthews is a Cybersecurity Analyst with experience in updating information Security System Policies and establishing baselines in accordance with NIST, FISMA, and other industry best practices. He has experience in performing vulnerability assessments to detect potential risks in single or multiple assets across an enterprise network. Mr. Matthews is also experienced in performing updates of IT security policies, procedures, standards, and guidelines per Federal requirements.

SCA WORK EXPERIENCE

SeNet International | Fairfax, VA | April 2019-Present

Mr. Matthews has been an employee of SeNet since April of 2019. Position on following SCA Projects: Cybersecurity Analyst
Years of SCA Experience: 3

Nevada Silver State Health Exchange and Minnesota Health Exchange (4/2019-6/2019)

- Assisted in the Minimum Accept Risk Standards for Exchanges (MARS-E) 2.0 control assessment in accordance with Generally Accepted Government Auditing Standards (GAGAS/Yellow Book) to determine whether effective IT security controls were in place
- Identified potential security risks, analyzed possible opportunities for improvements, and assisted in the issuance of Plans of Action and Milestones (POA&M).

POC: POC: Eric Watt: Sr. Project Manager; Phone: (971) 261-7777

Government Printing Office (GPO) (Present)

- Evaluated controls in place to protect the confidentiality, integrity, and availability of the GPO systems
- Updated the System Security Plans (SSP) and System Characterization Documents (SCD) in accordance with NIST, FISMA, FIPS, GAGAS and industry best security practices

POC: John Hannan, Director IT Security; Phone: (202) 512-1021

Minnesota Marketplace Exchange (MNSure) (9/2019-11/2019)

- Oversaw the security assessment task issued by GetInsured for the Minnesota Marketplace Exchange (MNSure) in which SeNet performed a security and privacy controls assessment. This contract includes performing a security assessment of the full control suite in the System Security Plan (SSP) for the MNSure web application in accordance with the Centers for Medicare and Medicaid Services (CMS) Minimum Acceptable Risk Standards for Exchanges (MARS-E 2.0) Security Assessment Control

POC: Deb Schierbaum, Manager, Data Operations and InfoSec; Phone: (253) 209-0082

Elijah Matthews

SCA EXPERIENCE *CONTINUED*

Cybersecurity Jr. Analyst

Kforce | Alexandria, VA | 09/2018-04/2019

- Developed, reviewed, and updated Information Security System Policies, established security baselines in accordance with NIST, FISMA, FIPS, and industry best security practices
- Performed vulnerability scanning with the support of the Nessus scanning tool to detect potential risks on a single or multiple assets across the enterprise network
- Updated IT security policies, procedures, standards, and guidelines per the respective department and Federal requirements
- Performed risk assessments, helped review and update POA&M, Security Control Assessments, Configuration Management Plans (CMP), Contingency Plans (CP), and Incident Response Plans (IRP) based on both internal requirements and industry best practices
- Performed Security Assessment and Authorization (SA&A) using NIST SP 800-53 Rev. 4/FIPS 200 (Security Controls) and NIST SP 800-53^a Rev. 4 (Assessing Security Controls)

IT Support Specialist

United States Army National Guard | Washington, DC | 03/2017-04/2019

- Performed Network and System Administration
- Assisted with solving technical issues within the system
- Kept network infrastructure up-to-date and secured
- Wrote and maintains network security policies and monitors compliance
- Identified and recommended needed and optimal infrastructure improvements
- Troubleshoot various network issues affecting solutions and collaborates with staff/outside vendors to resolve complex problems

IT Support Specialist (continued)

United States Army National Guard | Washington, DC | 03/2017-Present

- Analyzed software, hardware, and network systems for various transmission systems
- Configured and installed routers, switches, and wireless controllers
- Evaluated complex computer systems to assess vulnerability and risk

Information Assurance Analyst

EZ Shield, Inc. | Washington, DC | 02/2016-04/2018

- Used Nessus, WebInspect, and DbProtect technologies
- Operated Microsoft Windows systems
- Provided NIST, FISMA analysis
- Utilized Step 4 (Security Assessment) of the NIST Risk Management Framework (RMF)
- Assisted in updating IT security policies, procedures, standards, and guidelines according to department and Federal guidelines
- Participated in client interviews to determine the system's security posture
- Supported the Information Assurance (IA) team to conduct risk assessments, documentation for Security Control Assessment, as well as vulnerability testing and scanning
- Prepared and submitted Security Assessment Plan (SAP)

Jr. IT Security Analyst

Trusant Technologies, LLC. | 07/2014-02/2016



BULLETPROOF

a GLI company