CYBERSECURITY

Presented by: PSA SECURITY NETWORK

PLAYBOOK SERIES

RESOURCE GUIDE

TABLE OF CONTENTS

This Resource guide is intended to be a working document, with changes and additions being made as the cybersecurity playbook series develops.

Current Version-5.17.16

(ISC)2 - www.isc2.org

Mission:

Support and provide members and constituents with credentials, resources, and leadership to address cyber, information, software and infrastructure security to deliver value to society.

Certifications Offered

CAP - The Certified Authorization Professional (CAP) certification is an objective measure of the knowledge, skills and abilities required for personnel involved in the process of authorizing and maintaining information systems. Specifically, this credential applies to those responsible for formalizing processes used to assess risk and establish security requirements and documentation. Their decisions will ensure that information systems possess security commensurate with the level of exposure to potential risk, as well as damage to assets or individuals.

SSCP - The SSCP certification is the ideal credential for those with proven technical skills and practical security knowledge in hands-on operational IT roles. It provides industry-leading confirmation of a practitioner's ability to implement, monitor and administer IT infrastructure in accordance with information security policies and procedures that ensure data confidentiality, integrity and availability.

CISSP - The vendor-neutral CISSP certification is the ideal credential for those with proven deep technical and managerial competence, skills, experience, and credibility to design, engineer, implement, and manage their overall information security program to protect organizations from growing sophisticated attacks.

CCFP - The evolving field of cyber forensics requires professionals who understand far more than just hard drive or intrusion analysis. The field requires CCFP professionals who demonstrate competence across a globally recognized common body of knowledge that includes established forensics disciplines as well as newer challenges, such as mobile forensics, cloud forensics, anti-forensics, and more.

HCISSP - As the rapidly evolving healthcare industry faces increasing challenges to keeping personal health information protected, there is a growing need to ensure knowledgeable and credentialed security and privacy practitioners are in place to protect this sensitive information.

CCSP - Backed by the two leading non-profits focused on cloud and information security, the Cloud Security Alliance (CSA) and (ISC)², the CCSP credential denotes professionals with deep-seated knowledge and competency derived from hands-on experience with cyber, information, software and cloud computing infrastructure security. CCSPs help you achieve the highest standard for cloud security expertise and enable your organization to benefit from the power of cloud computing while keeping sensitive data secure.

CSSLP - Attackers and researchers continue to expose new application vulnerabilities, and it's no wonder that application vulnerabilities are ranked the #1 threat to cybersecurity professionals (according to the 2015 (ISC)² Global Information Security Workforce Study). Web application security must be a priority for organizations to protect their business and reputation. For this reason, it is crucial that anyone involved in the software development lifecycle (SDLC) be knowledgeable and experienced in understanding how to build secure software.

CompTIA www.comptia.org

CompTIA is the voice of the world's information technology (IT) industry. As a non-profit trade association, we advance the global interests of IT professionals and IT channel organizations and enable them to be more successful with industry-leading IT certifications and IT business credentials, IT education, resources and the ability to connect with like-minded, leading IT industry experts.

Certifications Offered

A+: CompTIA A+ covers PC hardware and peripherals, mobile device hardware, networking and troubleshooting hardware and network connectivity issues. It also covers installing and configuring operating systems including Windows, iOS, Android, Apple OS X and Linux. It also addresses security, the fundamentals of cloud computing and operational procedures.

Network+: CompTIA Network+ covers the configuration, management, and troubleshooting of common wired and wireless network devices. Also included are emerging technologies such as unified communications, mobile, cloud, and virtualization technologies.

Security+: CompTIA Security+ certification covers network security, compliance and operation security, threats and vulnerabilities as well as application, data and host security. Also included are access control, identity management, and cryptography.

Cloud+: CompTIA Cloud+ covers competency in cloud models, virtualization, infrastructure, security, resource management and business continuity.

Linux+: CompTIA Linux+ covers common tasks in major distributions of Linux, including the Linux command line, basic maintenance, installing and configuring workstations, and networking.

ISACA (Information Systems Audit and Control Association) www.issa.org

ISACA provides practical guidance, benchmarks and other effective tools for all enterprises that use information systems. Through its comprehensive guidance and services, ISACA defines the roles of information systems governance, security, audit and assurance professionals worldwide. The COBIT framework and the CISA, CISM, CGEIT and CRISC certifications are ISACA brands respected and used by these professionals for the benefit of their enterprises.

Certifications Offered

Certified Information Systems Auditor (CISA)

The CISA certification is world-renowned as the standard of achievement for those who audit, control, monitor and assess an organization's information technology and business systems.

Certified Information Security Manager (CISM)

The management-focused CISM is the globally accepted standard for individuals who design, build and manage enterprise information security programs. CISM is the leading credential for information security managers.

Certified in the Governance of Enterprise IT (CGEIT)

CGEIT recognizes a range of professionals for their knowledge and application of enterprise IT governance principles and practices. CGEIT provides you the credibility to discuss critical issues around governance and strategic alignment based on your recognized skills, knowledge and business experience.

Certified in Risk and Information Systems Control (CRISC)

CRISC (pronounced "see-risk") is the only certification that positions IT professionals for future career growth by linking IT risk management to enterprise risk management, and positioning them to become strategic partners to the business.

Cybersecurity Nexus – CSX Certificate and CSX-P Certification

As the cyber landscape continues to rapidly evolve, it's not enough to rely solely on knowledge and theory. A performance-based CSX certification is a testament to your real-life skills and experience and proclaims that your commitment, tenacity, and abilities exceed expectations. CSX programs and certifications help individuals demonstrate their skills and prove that they know the most current cyber security standards, and offer employers confidence that their employees are up to demanding tasks.

ISSA (Information Systems Security Association)

The Information Systems Security Association (ISSA)® is a not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications, and peer interaction opportunities that enhance the knowledge, skill, and professional growth of its members.

Program Offered

ISSA's Cyber Security Career Lifecycle™ (CSCL)

A program to enable professionals to steer their individual career paths by providing guidance and resources needed to achieve their long-term career goals. The CSCL is divided into 5 stages, with the opportunity for a variety of paths within each level

CSCL Levels and Descriptions

Pre-Professional: any individual who has not yet (and never has) obtained a position working in the cybersecurity field. This may include anyone who has interest in working in this area with or without formal training and education in the field. Examples of individuals and or situations who may be part of this phase are: individuals who are switching careers (former military, IT, retail, law enforcement, etc.) and students (high school or university).

Entry Level: An individual who has yet to master general cybersecurity methodologies/principles. Individuals in this phase of the lifecycle may have job titles such as; associate cybersecurity analyst, associate network security analyst, and cybersecurity risk analyst for example.

Mid-Career: An individual who has mastered general of security methodologies/principles and have determined their area of focus or specialty. Individuals in this phase of the lifecycle may have job titles such as; network security analyst, cybersecurity forensics analyst, application security engineer, network security engineer. Individuals who are nearing the "senior level", may begin to hold job titles such as senior network security engineer, senior cybersecurity analyst for example.

Senior Level: An individual who has extensive experience in cybersecurity and has been in the profession for 10+ years. These individuals have job titles such as senior cybersecurity risk analysis, principal application security engineer, director of cybersecurity, etc.

Security Leader: An individual who has extensive security experience, ability to direct and integrate security into an organization. These individuals have job titles such as Chief Information Security Officer, Chief Cybersecurity Architect, etc. After extensive periods of leadership – some become recognized industry leaders.

SANS Institute www.sans.org

SANS Institute is recognised as the global leader in computer and information security training. Founded in 1989 - as a cooperative research and education organisation - SANS programmes now reach more than 200,000 security professionals each week.

Certifications Offered

Global Information Assurance Certification (GIAC) is the leading provider and developer of Cyber Security Certifications. GIAC tests and validates the ability of practitioners in information security, forensics, and software security. GIAC certification holders are recognized as experts in the IT industry and are sought after globally by government, military and industry to protect the cyber environment.

Security Essentials (GSEC)

Security Professionals that want to demonstrate they are qualified for IT systems hands-on roles with respect to security tasks. Candidates are required to demonstrate an understanding of information security beyond simple terminology and concepts.

Incident Handler (GCIH)

Incident handlers manage security incidents by understanding common attack techniques, vectors and tools as well as defending against and/or responding to such attacks when they occur. The GCIH certification focuses on detecting, responding, and resolving computer security incidents and covers the following security techniques

Intrusion Analyst (GCIA)

GIAC Certified Intrusion Analysts (GCIAs) have the knowledge, skills, and abilities to configure and monitor intrusion detection systems, and to read, interpret, and analyze network traffic and related log files.

Penetration Tester (GPEN)

The GPEN certification is for security personnel whose job duties involve assessing target networks and systems to find security vulnerabilities. Certification objectives include penetration-testing methodologies, the legal issues surrounding penetration testing and how to properly conduct a penetration test as well as best practice technical and non-technical techniques specific to conduct a penetration test.

Web Application Penetration Tester (GWAPT)

Web applications are one of the most significant points of vulnerability in organizations today. Most organizations have them (both web applications and the vulnerabilities associated with them). Web app holes have resulted in the theft of millions of credit cards, major financial loss, and damaged reputations for hundreds of enterprises. The number of computers compromised by visiting web sites altered by attackers is too high to count. This certification measures and individuals understanding of web application exploits and penetration testing methodology. Check your web applications for holes before the bad guys do.

Perimeter Protection Analyst (GPPA)

The GIAC Certified Firewall Analyst (GCFW) certification has been renamed to the GIAC Certified Perimeter Protection Analyst (GPPA) effective January 1, 2014. This change comes as the industry continues to incorporate Cloud, mobile and virtualization into their systems, presenting new challenges into the traditional perimeter defenses. The GPPA addresses these challenges as well as traditional perimeter protection and multi-layered security.

Windows Security Administrator (GCWN)

GIAC Certified Windows Security Administrators (GCWNs) have the knowledge, skills and abilities to secure Microsoft Windows clients and servers, including technologies such as PKI, IPSec, Dynamic Access Control, Group Policy, RADIUS, BitLocker, and PowerShell.

Information Security Fundamentals (GISF)

Proficient infosec administrators can network well on the eight layer of the ISO model (political) and the material contained in this track will help them to bridge the gap that often exists between managers and system administrators. GISF candidates will learn and be able to demonstrate key concepts of information security including: understanding the threats and risks to information and information resources, identifying best practices that can be used to protect them, and learning to diversify our protection strategy.

Enterprise Defender (GCED)

The GCED builds on the security skills measured by the GSEC (no overlap). It assesses more advanced, technical skills that are needed to defend the enterprise environment and protect an organization as a whole. Knowledge, skills and abilities assessed are taken from the areas of Defensive Network Infrastructure, Packet Analysis, Penetration Testing, Incident Handling, and Malware Removal.

Assessing & Auditing Wireless Networks (GAWN)

The GAWN certification is designed for technologists who need to assess the security of wireless networks. The certification focuses on the different security mechanisms for wireless networks, the tools and techniques used to evaluate and exploit weaknesses, and techniques used to analyze wireless networks. Students will not only gain experience using tools to assess wireless networks, they will understand how the tools operate and the weaknesses in protocols that they evaluate.

Industrial Cyber Security Professional (GICSP)

The GICSP bridges together IT, engineering and cyber security to achieve security for industrial control systems from design through retirement. This unique vendor-neutral, practitioner focused industrial control system certification is a collaborative effort between GIAC and representatives from a global industry consortium involving organizations that design, deploy, operate and/or maintain industrial automation and control system infrastructure. GICSP will assess a base level of knowledge and understanding across a diverse set of professionals who engineer or support control systems and share responsibility for the security of these environments.

UNIX Security Administrator (GCUX)

GIAC Certified UNIX System Administrators (GCUXs) have the knowledge, skills and abilities to secure and audit UNIX and Linux systems.

Exploit Researcher & Advanced Penetration Tester (GXPN)

Security personnel whose job duties involve assessing target networks, systems and applications to find vulnerabilities. The GXPN certifies that candidates have the knowledge, skills, and ability to conduct advanced penetration tests, how to model the abilities of an advanced attacker to find significant security flaws in systems, and demonstrate the business risk associated with these flaws.

Mobile Device Security Analyst (GMOB)

Mobile phones and tablets continue to demonstrate their usefulness and importance in enterprises and government offices. With the amount of sensitive data that can be accessed on these devices and their lack of security, mobile devices are enticing targets for nefarious attackers.

Critical Controls Certification (GCCC)

GIAC Critical Controls Certification (GCCC) is the only certification based on the Critical Security Controls, a prioritized, risk-based approach to security. This certification ensures that candidates have the knowledge and skills to implement and execute the Critical Security Controls recommended by the Council on Cybersecurity, and perform audits based on the standard. Successful candidates must have a solid understanding of the philosophies and driving forces behind the creation of the Critical Security Controls, their scope, and how these controls can be used to prioritize information security controls based on community risk assessment efforts as well as understanding how the Critical Security Controls relate to other information assurance standards (such as ISO 27000, NIST 800-53, the NIST Core Framework, and others) and how the controls can be used to meet the goals of those standards. GCCC holders will make a practical and real difference in the security posture of any organization from a SMB to a multi-national corporation or governmental agency.

Continuous Monitoring Certification (GMON)

Preventing all intrusions is impossible, but early detection is a must for the security of your enterprise. The proper use of Defensible Security Architecture, Network Security Monitoring (NSM)/Continuous Diagnostics and Mitigation (CDM)/ Continuous Security Monitoring will support the hindrance of intrusions and allow for early detection of anomalous activity.

Python Coder (GPYC)

A professional that can create and modify custom tools is a valuable member of any information security team. Code developers with information security skills can customize tools to their environment, create tools for the information security community, increase productivity by automating previously manual tasks, simulate advanced attacks, and more. The GPYC certification focuses on applying core programming concepts and techniques to the Python programming language. The certification has a special focus on skills and techniques that will assist an information security professional in penetration tests, daily work, and special projects. Certified individuals can create simple Python-based tools to interact with network traffic, create custom executables, test and interact with databases and websites, and parse logs or sets of data.

Cybrary www.cybrary.it

Training Program Offered

OUR REVOLUTION We believe IT and Cyber Security training should be free, for everyone, forever. We believe that everyone, everywhere, deserves the OPPORTUNITY to learn, primarily because everyone is essentially forced to use internet enabled devices. However, we are not prepared to defend ourselves against the cyber threats that exist and are emerging. Join the free Cyber Security training revolution at Cybrary.

BlackHat www.blackhat.com

Training Event Offered

2016 - Black Hat - built by and for the global InfoSec community - returns to Las Vegas for its 19th year. This six day event begins with four days of intense Trainings for security practitioners of all levels (July 30 - August 2) followed by the two-day main event including over 100 independently selected Briefings, Business Hall, Arsenal, Pwnie Awards, and more (August 3-4).

Course Examples: Adaptive Penetration Testing, Metasploit Basic, Metasploit Mastery, Advanced Hardware Hacking, Advanced Infrastructure Hacking, Advanced Social Engineering

Titan Info Security Group: http://www.psasecurity.com/services/business-solutions/titaninfosecurity

Employing legal, cyber security and risk management expertise to help you assess how data is secured and develop a plan to lower your risk of a breach, reduce the liability after a breach, protect your reputation, and prepare for that inevitable breach. Understand the vulnerabilities, threats, and overall risks to your organization and data so you can effectively prepare and implement a plan that lowers the risk of a data breach, reduces or eliminates your liability, protects your reputation and allows you to quickly detect a data breach and recover quickly.Take control of your security now!

SecureXperts: http://www.psasecurity.com/services/business-solutions/securexperts/

SecureXperts provides an affordable portfolio of services to companies that are either looking to begin or to evaluate their existing cyber security program. It does not have to be an uphill battle.
SecureXperts works together with your company to understand assess and re-align your company's infrastructure, products and services to insure cyber security. We begin by helping you to create and paint the road map that best works for your organization.

BB&T:http://www.psasecurity.com/services/business-solutions/bbt-insurance/

Your insurance program should be customized to effectively provide your company's risk management needs. To ensure your risk management program is tailored for each franchisee's needs, BB&T Insurance Services will work with you to develop a program that provides not only necessary coverage, but additional coverage to ensure your business will recover quickly following a claim.
BB&T Insurance Services works with you all year, instead of just at renewal time, to assist with any insurance concerns or questions that may arise. We also provide assistance with contract review for insurance requirements, aggressive workers' compensation cost management, assistance with safety program development and aggressive claims management.
As one of the largest independent insurance agencies, we'll represent your best interests as we objectively select competitively priced coverage from leading insurers. Your program will feature: individually underwritten insurance policies; loss control services, including facility inspections, interim loss control reviews and safety seminars; fast and efficient claims response by experienced adjusters; and flexible financing and payment options for premium payments.

Synnex: http://www.synnex.com/servicesolv/solutions/index.html

SYNNEX SERVICESolv makes it easy to navigate the broad array of service options available to you. We've segmented our overall service offering into three distinct segments related to specific aspects of the IT lifecycle. Leverage any or all of these offerings to expand your business into new areas, build a new services-based model, or fill in gaps in your capabilities to take on a project that is outside your normal ability to accept.

CSR Professional Services: http://www.psasecurity.com/services/business-solutions/csr-professional-services/

CSR is the leading provider of data life cycle management, compliance solutions and expert services to hundreds of thousands of businesses domestically and around the world. We enable compliance with Personally Identifiable Information (PII) requirements,while facilitating best practices to reduce the business risk and financial liability associated with the acquisition, handling, storage, sharing and disposal of data.

IDmachines: http://www.idmachines.com

IDmachines provide design, integration and business consulting services.
IDmachines' 30 years of experience in large scale identity, automation, security and technology programs helps our customers accelerate their understanding and use of modern credentials and identity infrastructure.
IDmachines brings integrity, policy and technology subject matter expertise to its activity. Our identity, credential, access and security system assessment, design and integration works with standards based commercial off-the-shelf (COTS) architectures and solutions to register, enroll, issue and use most types of contact, contactless and other tokens. Recognized subject matter expertise on Federal Information Processing Standard 201 (FIPS 201) and Personal Identity Verification Interoperability (PIV-I) and identity, credential and access management (ICAM) infrastructure, applications and devices.

Smithee, Spelvin, Agnew & Plinge Kroll: http://www.smithee.us/

Smithee, et al. provides consulting services specializing in software engineering and risk management for converged infrastructures supporting the vendor supply chain from end user and integrators to manufacturers and suppliers.

Knowbe4: https://www.knowbe4.com/

KnowBe4 delivers 'new-school' security awareness training combined with set-it-and-forget-it simulated phishing attacks for an extremely effective user education program.
With this world-class, user-friendly and effective Internet Security Awareness Training, KnowBe4 provides self-service enrollment, and both pre-and post-training phishing security tests that show the percentage of end-users that are Phish-prone. KnowBe4's unique "double-random" scheduled Phishing Security Tests keep employees on their toes with security top of mind, and can provide instant remedial online training in case an employee falls for a simulated phishing attack.

Cylance: https://www.cylance.com/

Cylance® is revolutionizing cybersecurity with products and services that proactively prevent, rather than reactively detect the execution of advanced persistent threats and malware. Our technology is deployed on over 4 million endpoints and protects hundreds of enterprise clients worldwide including Fortune 100 organizations and government institutions.

Wombat Security: https://www.wombatsecurity.com/

Wombat Security Technologies, headquartered in Pittsburgh, PA, provides information security awareness and training software to help organizations teach their employees secure behavior. Our Security Education Platform includes integrated knowledge assessments, a library of simulated attacks, and interactive training modules, which have been proven to reduce successful phishing attacks and malware infections by up to 90%.

What is Cyber Risk?

Cyber Risk derives from use of the Internet as a tool to conduct e-commerce and general business operations. Common exposures include (but are not limited to):

- data/security breach
- copyright or trademark infringement
- data destruction and/or corruption as a result of a virus
- cyber extortion
- hackers, worms and other cyber meddlers
- firewall and network security attacks

Why should I buy Cyber Risk Insurance?

If your business uses the Internet, it is exposed to risk that may not be covered under your current commercial insurance policy. In fact, typical General Liability policies often do not cover activities associated with Website Publishing or Network Security. If lack of coverage from existing policies is not enough encouragement for you to purchase Cyber Risk Insurance, then consider the following statistics:

- The average per record cost of a data breach is $201 per customer record. Lost business now accounts for 69% of data breach costs.
- According a national survey, many businesses do not have the tools or procedures in place to detect identity fraud, including an incident response plan, vendor management procedures or data encryption for personally identifiable information.
- Most victims do not even know that their data was compromised. 87% of the breaches were discovered by a third party.2
- 92% of breaches were from external sources. Over 80% from overseas, organized crime accounts for 55% of external breaches.
- There are Regulatory Requirements that apply to most organizations today. Data Breach Notification Laws are in effect in most states today that require notification of customers in the event of a data breach. The Red Flags Rule is being enforced by the Federal Trade Commission (FTC) that requires organizations to have Identity Theft Protection Programs in place (or be subject to penalties or fines). The compliance costs to notify customers as well as the risk of incurring fines/penalties can drive up business costs.

What is the Cost of Cyber Risk Insurance?

The cost is calculated using a number of criteria, including, but not limited to, the nature of your operations, size of operations (Revenues) and the coverage components, as well as if purchased independently of, or combined with any other commercial insurance options such as general liability and property coverage.

Cybersecurity Insurance Application Example Questionnaire

Please answer all the questions on this form. Before any question is answered please carefully Read, then sign, the declaration at the end of the application form. Underwriters will rely on the statements that you make on this form. In this context, any insurance Coverage that may be issued based upon this form will be void if the form contains falsehoods, misrepresentations, or omissions. Please therefore ensure your responses to the questions in the form are complete and correct.

Any policy that may be issued based upon this form will provide claims first made and reported coverage.

Section 1 – Your Details

1. Applicant(s):
2. Address:
3. Contact name and title of individual responsible to executive management for information Security operations:
4. Contact's telephone number and email address:
5. Names of all subsidiary companies (if any):
6. Please detail any mergers and acquisitions undertaken in the last 3 years (including retro-dates):

Name of Entity: Retro Date:

7. Website home page (including subsidiaries):

Section 2 – Your Business

8. Date established:
9. Total number of staff:
10. Detailed description of business / Professional Services:
11. Identify your corporate structure (C Corp, Partnership, S Corp LLC, Other):
12. Please confirm the total revenues
    a) from your most recent financial year;
    b) projected for your next financial year.
13. Please confirm the total revenues from your Internet activities only
    a) for your most recent financial year;
    b) projected for your next financial year.

14. Do you have any customers that represent more than 50% of your revenue: Yes No

15. Please list all URL addresses for all public-facing websites that are to be insured:

Section 3 – Your Professional Services

Please complete this section for Technology Errors and Omissions coverage

16. Please provide an analysis of your revenue (by percentage) from the following:

TECHNOLOGY PRODUCTS AND SERVICES PROVIDED TO THIRD PARTIES
Customized development
Pre-packaged/Shrink Wrap
Consulting Implementation/Integration
Real Time Production
Real Time Trading
Enterprise Resource Planning
Procurement Distribution
Sales Training
Other Technology Products or Services Description
Other Technology Products or Services Description:

NON-TECHNOLOGY PRODUCTS OR SERVICES SOLD TO THIRD PARTIES

Healthcare
Financial
Media, Advertising, Entertainment
Wholesaler or Retailer of Products Manufacturing
Non-Profit Education
Non Tech.
Other-Describe Non Tech.
Other-Describe

17. Please identify your mission critical suppliers:

18. Do you or will you within the next twelve (12) months perform any of the following activities (whether through a hosted website, your own website or by your customers using products or services provided by you):

i) Storage of customer/subscriber names and addresses Yes No

ii) Storage of credit/debit card numbers Yes No

iii) Storage of credit history and ratings Yes No

iv) Storage of medical records or personal health information Yes No

v) Storage of intellectual property of others Yes No
If yes, please give details:

vi) Storage or access to bank records/investment data or financial transactions of subscribers/customers Yes No

vii) Storage or other customer/subscriber information Yes No

If yes, please give details:

viii) Electronic publishing, marketing, dissemination or distribution of copyrighted material of Others Yes No

ix) Electronic publishing, marketing, dissemination or distribution of original works Yes No

Do you provide content for third party web sites? Yes No

x) Electronic publishing, marketing, dissemination or distribution of pornography or adult entertainment material Yes No

xi) Advertising the products or services of other companies on websites, via email or other electronic means for a fee or commission Yes No

xii) Provide legal, financial or personal finance advice Yes No

xiii) Provide medical or health advice Yes No

xiv) Provide other personal advice services such as counselling Yes No

xv) Provide website services or products to international customers/subscribers (including web-hosting or ISP) Yes No

If yes, please give details:

xvi) Registration of Domain Names for others (Domain Registrar) Yes No

xvii) Sell or share individual subscriber or user identifiable information with another company Yes No

19. Please indicate the end-user application of your company's products/services by market sector:

Market Sector	Revenue by percentage
Aerospace	
Agriculture	
Communications/Telecommunications	
Construction	
Educational Institutions	
Financial Institutions	
Government Healthcare	
Medical Home Use	
Industrial/Manufacturing Use	
Trade/Commerce	
Retail/wholesale Other (please detail)	
Other (please detail)	

Section 4 – Your Website

Please complete for your Internet operations (if applicable)
The information provided here will be supplemented by an online Network Security Assessment

20. Does your website contain materials designed to be downloaded? Yes No
If yes, please give details:

21. Does your company have an established procedure for editing or removing from your Web site or Internet Service libellous or slanderous content, or content that infringes the Intellectual Property rights of others (copyright, trademark, trade name, trade secrets etc.)?
Yes No

If yes, please confirm whether this review procedure is carried out by a qualified attorney.
Yes No

22. Does your company use material provided by others, such as content, music, graphics, and video streams, in your software, or on your website?

Yes No

If yes, please confirm whether you obtain written licences and consent agreements for the use of these materials:

Yes No

23. Does your company use the Internet or an intranet for political, fundraising or cause activities: for gambling; for pornography; or for the sale of prohibited, regulated or restricted items such as tobacco, other drugs or liquor, or fire arms?

Yes No

If yes, please give details:

Section 5 – Your IT systems

Please complete for your network
The information provided here may be supplemented by an online Network Security Assessment

24. Do you use Microsoft Operation System environments for your public-facing systems and/or services, such as IIS (web server), or other Microsoft Operating Systems servers for database, email or DNS.

Yes No

If yes, do you have a formal patch management process in place and have you installed the latest available security vulnerability alert and service pack? Yes No

25. Is firewall technology used at all Internet points-of-presence to prevent unauthorized access?

Yes No

26. Does your company use anti-virus software on all desktops/portable computer devices and mission-critical servers and is it updated in accordance with the software provider's requirements?

Yes No

27. Are system backup and recovery procedures documented and tested for all mission-critical systems?

Yes No

28. Does your company have a written policy on Email and Internet use?

Yes No

29. Does your company have a published information security policy, and is there an organizational manager who is directly responsible for information security compliance operations?
Yes No

30. Are there regular security reviews of IT systems by internal audit personnel or a trusted third party? Yes No

Section 6 – Your Risk Mitigation

31. Does your company use Independent Contractors to whom you sub-contract work?
Yes No

If yes, please confirm whether you require Independent Contractors to carry professional liability insurance, and provide a description of any indemnities, hold harmless agreements etc:

32. If Yes to 31 above:

Does your company always use a written contract upon engagement of such Independent Contractors?
Yes No

A. If Yes, please attach a copy.

B. If No or Not always, please describe how you agree the scope of the contract with your customer:

Please provide a copy of your standard customer contract with your application.

33. Within the last two (2) years, have any customers either failed to pay for or requested a refund for a product or service you provided due to an alleged problem? (whether due to non-performance, dissatisfaction or otherwise) Yes No

34. Has your company ever been declined for Errors and Omissions, Professional Liability or Media Liability insurance or had an existing policy cancelled? Yes No

If yes, please explain:

Privacy Supplemental

36. Have you indentified all relevant regulatory and industry compliance frameworks that are applicable to the organization? Yes No
(Please provide details of compliance applicable to your organization, with details of the latest audit carried out)

37. Is all sensitive and confidential information that is transmitted within and from your organization encrypted using Industry-grade mechanisms? Yes No

38. Do you have strict user revocation procedures on user accounts and inventoried recovery of all information assets following employment termination? Yes No

39. Do you have established procedures for ensuring the deletion of all sensitive data from systems and devices prior to their disposal from the company? Yes No

40. Is all sensitive and confidential information stored on your organization's databases, servers and data files encrypted? Yes No

41. Are access control procedures and hard drive encryption in force to prevent unauthorized exposure of data on all Laptops/ Blackberry's, and home based PC's? Yes No

42. Do you ensure that all wireless networks have protected access? Yes No

43. In response to California's SB 1386 and other similar laws have you established a procedure for determining the severity of a potential data security breach and a notification procedure to all individuals who may be adversely affected by such exposures?
Yes No

44. Has the organization ever sustained a significant system intrusion, tampering, virus or malicious code attack, loss of data, hacking incident, data theft or similar?
Yes No

45. Do you store credit card details on your network or does it go straight off to the payment processor? Yes No

46. Have you specifically checked that your SQL servers with credit card details are programmed to prevent SQL injection attacks? Yes No

47. Is your credit card data on your SQL server always encrypted? Yes No

48. Is all Personally Identifiable Information (PII) encrypted at rest and in transit?
Yes No

49. Is all Personally Identifiable Information (PII) encrypted on the network and off the network including remote devices, i.e. laptops, blackberries, disks, etc.
Yes No

50. Are all back up tapes / cassettes secure in transit? Are they picked up, shipped, and stored by reputable third parties? Yes No

51. Please provide brief details of the impact on your business in the event that your network or applications should fail or be compromised?

52. Is the operation and connectivity of your computer network business critical and if so how many hours would it have a material effect on your business?

53. Please comment on recovery/ contingency plans in place to avoid business interruption due to IT systems failure, and/ or alternative working procedures (interdependency, outsourcing, alteration of process, additional employment, redundant servers etc)

54. Is this plan regularly tested and updated? Yes No

55. Please provide full details of Personally Identifiable Information, numbers and types etc?

56. Please provide further details of how they store credit cards details(if applicable) (numbers, encryption etc) both on network and point of sale?

57. Please provide the estimated number of records stored that contain personally identifiable information.

58. * If you transmit/store payment card data, have you confirmed your compliance with the most recent PCI Data Security Standards: Yes No

Regarding your Claims or Incidents that may give Rise to a Claim

59. During the past three years, has anyone made any Claim against the Applicant for invasion of or interference with any right of privacy, wrongful disclosure of personal information, or violation of any privacy related statute or regulation? Yes No

If yes, please detail separately and include any pending or prior incident, event or litigation providing full details of all relevant facts:

60. In the last 5 years has your company been the subject of any cease and desist orders or been the subject of official admonishments, critical directives or comments by regulators?
Yes No

If yes, please detail separately and include any pending or prior incident, event or litigation providing full details of all relevant facts:

61. In the last 5 years has your company experienced any claims or are you aware of any circumstances that could give rise to a claim that would have been covered by this policy?
Yes No

If yes, please detail separately and include any pending or prior incident, event or litigation providing full details of all relevant facts:

Declaration

I hereby declare that I am authorized to complete this application on behalf of the applicant and that after due inquiry, to the best of my knowledge and belief, the statements and particulars in this application are true and complete and no material facts have been misstated, suppressed, or omitted. I undertake to inform underwriters or any alteration or addition to these statements or particulars which occur before or during any contract of insurance based on the applications is effected. I also acknowledge that this application (together with any other information supplied to underwriters) shall be the basis of such contract.

I understand that underwriters will rely on the statements that I make on this form. In this context, any insurance coverage that may be issued based upon this form will be void if the form contains falsehoods, misrepresentations or omissions.

Access Ability to make use of any information system (IS) resource.

Access Control Process of granting access to information system resources only to authorized users, programs, processes, or other systems.

Accreditation Formal declaration by a Designated Approving Authority that an Information System is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.

Activation Data Private data, other than keys, that are required to access cryptographic modules (i.e., unlock private keys for signing or decryption events).

Agency Any department, subordinate element of a department, or independent organizational entity that is statutorily or constitutionally recognized as being part of the Executive Branch of the Federal Government.

Agency CA A CA that acts on behalf of an Agency, and is under the operational control of an Agency.

Applicant The subscriber is sometimes also called an "applicant" after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed.

Archive Long-term, physically separate storage.

Attribute Authority An entity, recognized by the Federal PKI Policy Authority or comparable Agency body as having the authority to verify the association of attributes to an identity.

Audit Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.

Audit Data Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event.

Authenticate To confirm the identity of an entity when that identity is presented.

Authentication Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.

Backup Copy of files and programs made to facilitate recovery if necessary.

Binding Process of associating two related elements of information.

Biometric A physical or behavioral characteristic of a human being.

Certificate A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its subscriber, (3) contains the subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it. As used in this CP, the term "Certificate" refers to certificates that expressly reference the OID of this CP in the "Certificate Policies" field of an X.509 v.3 certificate.

Certification Authority (CA) An authority trusted by one or more users to issue and manage X.509 Public Key Certificates and CARLs or CRLs.

Certification Authority Revocation List (CARL) A signed, time-stamped list of serial numbers of CA public key certificates, including cross-certificates, that have been revoked.

CA Facility The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation.

Certificate A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies it's Subscriber, (3) contains the Subscriber's public key, (4) identifies it's operational period, and (5) is digitally signed by the certification authority issuing it.

Certificate Management Authority (CMA) A Certification Authority or a Registration Authority.

Certification Authority Software Key Management and cryptographic software used to manage certificates issued to subscribers.

Certificate Policy (CP) A Certificate Policy is a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.

Certification Practice Statement (CPS) A statement of the practices that a CA employs in issuing, suspending, revoking and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this CP, or requirements specified in a contract for services).

Certificate-Related Information Information, such as a subscriber's postal address, that is not included in a certificate. May be used by a CA managing certificates.

Certificate Revocation List (CRL) A list maintained by a Certification Authority of the certificates which it has issued that are revoked prior to their stated expiration date.

Certificate Status Authority A trusted entity that provides on-line verification to a Relying Party of a subject certificate's trustworthiness, and may also provide additional attribute information for the subject certificate.

Client (application) A system entity, usually a computer process acting on behalf of a human user, that makes use of a service provided by a server.

Common Criteria A set of internationally accepted semantic tools and constructs for describing the security needs of customers and the security attributes of products.

Compromise Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.

Computer Security Objects Registry (CSOR) Computer Security Objects Registry operated by the National Institute of Standards and Technology.

Confidentiality Assurance that information is not disclosed to unauthorized entities or processes.

Cross-Certificate A certificate used to establish a trust relationship between two Certification Authorities.

Cryptographic Module The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module.

Cryptoperiod Time span during which each key setting remains in effect.

Data Integrity Assurance that the data are unchanged from creation to reception.

Digital Signature The result of a transformation of a message by means of a cryptographic system using keys such that a Relying Party can determine: (1) whether the transformation was created using the private key that corresponds to the public key in the signer's digital certificate; and (2) whether the message has been altered since the transformation was made.

Dual Use Certificate A certificate that is intended for use with both digital signature and data encryption services.

Duration A field within a certificate that is composed of two subfields; "date of issue" and "date of next issue".

E-commerce The use of network technology (especially the internet) to buy or sell goods and services.

Encrypted Network A network on which messages are encrypted (e.g. using DES, AES, or other appropriate algorithms) to prevent reading by unauthorized parties.

Encryption Certificate A certificate containing a public key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes.

End Entity Relying Parties and Subscribers.

Federal Bridge Certification Authority (FBCA) The Federal Bridge Certification Authority consists of a collection of Public Key Infrastructure components (Certificate Authorities, Directories, Certificate Policies and Certificate Practice Statements) that are used to provide peer to peer interoperability among Agency Principal Certification Authorities.

Federal Bridge Certification Authority Membrane The Federal Bridge Certification Authority Membrane consists of a collection of Public Key Infrastructure components including a variety of Certification Authority PKI products, Databases, CA specific Directories, Border Directory, Firewalls, Routers, Randomizers, etc.

FBCA Operational Authority The Federal Bridge Certification Authority Operational Authority is the organization selected by the Federal Public Key Infrastructure Policy Authority to be responsible for operating the Federal Bridge Certification Authority.

Federal Public Key Infrastructure Policy Authority (FPKI PA) The Federal PKI Policy Authority is a federal government body responsible for setting, implementing, and administering policy decisions regarding interagency PKI interoperability that uses the FBCA.

Firewall Gateway that limits access between networks in accordance with local security policy.

High Assurance Guard (HAG) An enclave boundary protection device that controls access between a local area network that an enterprise system has a requirement to protect, and an external network that is outside the control of the enterprise system, with a high degree of assurance.

Information System Security Officer (ISSO) Person responsible to the designated approving authority for ensuring the security of an information system throughout its lifecycle, from design through disposal.

Inside Threat An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.

Protection against unauthorized modification or destruction of information. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.

Intellectual Property Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.

Intermediate CA A CA that is subordinate to another CA, and has a CA subordinate to itself.

Key Escrow A deposit of the private key of a subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the subscriber, the terms of which require one or more agents to hold the subscriber's private key for the benefit of the subscriber, an employer, or other party, upon provisions set forth in the agreement. [adapted from ABADSG, "Commercial key escrow service"]

Key Exchange The process of exchanging public keys in order to establish secure communications.

Key Generation Material Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.

Key Pair Two mathematically related keys having the properties that (1) one key can be used to encrypt a message that can only be decrypted using the other key, and (ii) even knowing one key, it is computationally infeasible to discover the other key.

Local Registration Authority (LRA) A Registration Authority with responsibility for a local community.

Memorandum Agreement between the Federal PKI Policy Authority and an Agency allowing Memorandum of Agreement (MOA) interoperability between the Agency Principal CA and the FBCA.

Mission Support Information Information that is important to the support of deployed and contingency forces.

Mutual Authentication Occurs when parties at both ends of a communication activity authenticate each other (see authentication).

Naming Authority An organizational entity responsible for assigning distinguished names (DNs) and for assuring that each DN is meaningful and unique within its domain.

National Institute of Standards and Technology (NIST) Organization responsible for developing cyber security standards for US Federal and Defense Organizations.

Non- Repudiation Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. Technical non-repudiation refers to the assurance a Relying Party has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding private signature key. Legal non-repudiation refers to how well possession or control of the private signature key can be established.

Object Identifier (OID) A specialized formatted number that is registered with an internationally recognized standards organization. The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the federal government PKI they are used to uniquely identify each of the four policies and cryptographic algorithms supported.

Out-of-Band Communication between parties utilizing a means or method that differs from the current method of communication (e.g., one party uses U.S. Postal Service mail to communicate ith another party where current communication is occurring online).

Outside Threat An unauthorized entity from outside the domain perimeter that has the potential to harm an Information System through destruction, disclosure, modification of data, and/or denial of service.

Physically Isolated Network A network that is not connected to entities or systems outside a physically controlled space.

PKI Sponsor Fills the role of a Subscriber for non-human system components that are named as public key certificate subjects, and is responsible for meeting the obligations of Subscribers as defined throughout this CP.

Policy Management Authority (PMA) Body established to oversee the creation and update of Certificate Policies, review Certification Practice Statements, review the results of CA audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate policies. For the FBCA, the PMA is the Federal PKI Policy Authority.

Principal CA The Principal CA is a CA designated by an Agency to interoperate with the FBCA. An Agency may designate multiple Principal CAs to interoperate with the FBCA. Privacy Restricting access to subscriber or Relying Party information in accordance with Federal law and Agency policy. Private Key (1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.

Public Key (1) The key of a signature key pair used to validate a digital signature. (2) The key of 51 an encryption key pair that is used to encrypt confidential information. In both cases, this key is made publicly available normally in the form of a digital certificate

Public Key Infrastructure (PKI) A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.

Registration Authority (RA) An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a Registration Authority is delegated certain tasks on behalf of an authorized CA).

Re-key (a certificate) To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate on the new public key.

Relying Party A person or Agency who has received information that includes a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them.

Renew (a certificate) The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.

Repository A database containing information and data relating to certificates as specified in this CP; may also be referred to as a directory.

Responsible Individual A trustworthy person designated by a sponsoring organization to authenticate individual applicants seeking certificates on the basis of their affiliation with the sponsor.

Revoke a Certificate To prematurely end the operational period of a certificate effective at a specific date and time.

Risk An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.

Risk Tolerance The level of risk an entity is willing to assume in order to achieve a potential desired result.

Root CA In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.

Server A system entity that provides a service in response to requests from clients.

Signature Certificate A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.

Subordinate CA In a hierarchical PKI, a CA whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA (See superior CA)

Subscriber A Subscriber is an entity that (1) is the subject named or identified in a certificate issued to that entity, (2) holds a private key that corresponds to the public key listed in the certificate, and (3) does not itself issue certificates to another party. This includes, but is not limited to, an individual or network device.

Superior CA In a hierarchical PKI, a CA who has certified the certificate signature key of another CA, and who constrains the activities of that CA. (See subordinate CA).

System Equipment A comprehensive accounting of all system hardware and software types and settings.

Technical non-repudiation The contribution public key mechanisms to the provision of technical evidence supporting a non-repudiation security service.

Threat Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service.

Trust List Collection of trusted certificates used by Relying Parties to authenticate other certificates.

Trusted Agent Entity authorized to act as a representative of an Agency in confirming Subscriber identification during the registration process. Trusted Agents do not have automated interfaces with Certification Authorities.

Trusted Certificate A certificate that is trusted by the Relying Party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a "trust anchor".

Trusted Timestamp A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.

Trustworthy System Computer hardware, software and procedures that: (1) are reasonably secure from intrusion and misuse; (2) provide a reasonable level of availability, reliability, and correct operation; (3) are reasonably suited to performing their intended functions; and (4) adhere to generally accepted security procedures.

Update (a certificate) The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate.

1. NIST Risk Management Framework (April1, 2014)

http://csrc.nist.gov/groups/SMA/fisma/framework.html

The selection and specification of security controls for an information system is accomplished as part of an organization-wide information security program that involves the ***management of organizational risk***---that is, the risk to the organization or to individuals associated with the operation of an information system. The management of organizational risk is a key element in the organization's information security program and provides an effective framework for selecting the appropriate security controls for an information system---the security controls necessary to protect individuals and the operations and assets of the organization.

2. NIST Cyber Security Framework (Updated March 15, 2016)

http://www.nist.gov/cyberframework/

Created through collaboration between industry and government, the Framework consists of standards, guidelines, and practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable, and cost-effective approach of the Framework helps owners and operators of critical infrastructure to manage cybersecurity-related risk.

3. SANS Critical Security Controls (October 15, 2015)

http://www.sans.org/critical-security-controls

Note: Five "quick wins" delineated in Critical Controls 2, 3, and 4 (with one repeated in Control 12) are highlighted as the "First Five." They are being implemented first by the most security-aware and skilled organizations because they are the most effective means yet found to stop the wave of targeted intrusions that are doing the greatest damage to many organizations. The "First Five" cover (1) software white listing, (2) secure standard configurations, (3) application security patch installation within 48 hours, (4) system security patch installation within 48 hours, and (5) ensuring administrative privileges are not active while browsing the web or handling email. Most organizations monitor the coverage and effectiveness of these sub-controls through Continuous Monitoring and Mitigation as outlined in Critical Control 4.

4. Center for Internet Security Controls Version 6 (October 15, 2015)

https://www.cisecurity.org/critical-controls/download.cfm?f=CSC-MASTER-VER%206.0%20CIS%20Critical%20Security%20Controls%2010.15.2015

The Controls take the best-in-class threat data and transform it into actionable guidance to improve individual and collective security in cyberspace. Too often in cybersecurity, it seems the "bad guys" are better organized and collaborate more closely than the "good guys." The Controls provide a means to turn that around.

5. The Importance of Security Awareness Training (SANS Whitepaper)

http://www.sans.org/reading-room/whitepapers/awareness/importance-security-awareness-training-33013

6. Publication Citation: Building an Information Technology Security Awareness and Training Program http://www.nist.gov/manuscript-publication-search.cfm?pub_id=151287

7. NIST Security and Privacy Controls for Federal Information Systems and Organizations http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf