EXHIBIT A – Detailed Scope of Services

EXHIBIT A – Detailed Scope of Services

Roger Colón Jr.

Function and Specialization
Subject Matter Expert

- Information Assurance
- Security Awareness & Training
- Information Security
- Penetration/Vulnerability Testing

Clearance
Internal Revenue Service (IRS) Minimum Background Investigation (MBI)
Public Trust – Moderate (5C)
Public Trust – High Risk (6C)

Certification(s)
CompTIA A+ and Security+ – 2001 and 2005
DISA Systems Administrator – 2002
ISC^2 Certified Information System Security Professional (CISSP) – 2007
Certified Secure Software Lifecycle Professional (CSSLP) – 2009
Certified FISMA Compliance Practitioner (CFCP) – 2010
Core Impact Certified Professional (CICP) – 2009
IT Infrastructure Library (ITIL) v3 – 2010
Certified Information Security Manager (CISM) – 2017
Certified Ethical Hacker (CEH) – 2017
Certificate of Cloud Security Knowledge (CCSK) – 2019

Background
Mr. Colón is a highly experienced and certified Information Technology (IT), information security, information assurance, and cyber security engineer, ethical hacker, and IT auditor with over 20 years of experience, to include significant experience in building and managing cyber security programs, systems, and applications. Other significant experience in security architecture, engineering, security testing, and assessing security-related controls. Operational experience includes monitoring, auditing, pen testing, vulnerability management, delivering security awareness & training, and developing security-related documentation.

Experience
JANUS Software, Inc. (d/b/a JANUS Associates) **August 2016 – Present**
Senior Security Engineer

- Performs government assessments to determine security risks of JANUS clients.
- Assists commercial and healthcare entities to improve security.
- Performs HIPAA gap analyses, compliance reviews, and assessments for government entities.
- Conducts network analyses to determine security issues, performance, and how to re-architect for the future.
- Performs security assessments for wide range of JANUS clients.

Advanced Threat Analysis, Inc. (ATA) **2012 – February 2016**
Senior Penetration Tester/Senior Security Engineer

- Senior information security consultant for the federal and commercial sectors: Provided security engineering, cyber security event log monitoring, program management, IT auditing, implementation management, risk management, security controls assessments, vulnerability management, and penetration testing support on major applications, systems, and mobile technology.
- Utilized the following laws, or guidance when delivering consulting services: Federal Information Systems Management Act (FISMA), National Institute of Standards and Technology (NIST), DoD Information Assurance Certification and Accreditation Process (DIACAP), Open Web Application Security Project (OWASP), Office of Management and Budget (OMB) Circular A-123, Federal Information Processing Standard (FIPS), Payment Card Industry (PCI); Federal Information Systems Controls Audit Manual (FISCAM), Health Insurance Portability and Accountability Act (HIPAA), and Sarbanes-Oxley (SOX).
- Conducted Security Controls Assessments (SCA), IT auditing, vulnerability scanning, network, wireless, and web application penetration testing for the Internal Revenue Service (IRS), Department of Justice's (DOJ) Executive Office for United States Attorneys (EOUSA), National Oceanic and Atmospheric Administration (NOAA) Security Operations Center (SOC) and Network Operations Center (NOC), Centers for Medicare & Medicaid Services (CMS), Department of Energy (DOE), Veterans

Education

George Washington University Master Certificate, IT Project Management – 2010

American Intercontinental University, Master of Science, IT Management – 2004

University of Phoenix, Bachelor of Science, Information Systems – 2002

Anne Arundel Community College, Associate of Arts, Spanish – 2000

Administration (VA), M&T Bank, EMC, Community First Fund (CFF), Department of Homeland Security (DHS), and United States Bank.

- Conducted manual web application, and manual infrastructure penetration testing. Utilized industry best practices and research to exploit vulnerabilities with automated and manual techniques.
- Utilized commercial and open source solutions to conduct automated vulnerability scanning and penetration testing. Scanned web applications and general support systems for vulnerabilities.
- Developed penetration test reports for customers.
- Briefed upper management on issues identified on their systems or with their processes.
- Developed the Rules of Engagement (ROE) and obtained organization approval before conducting any pen testing or ethical hacking; ROE included tool set and scripts to be used during the assessment/testing.
- Performed threat modeling and identify architectural risks that can be exploited through penetration testing.
- Based on research and industry best practices, developed Standard Operating Procedures (SOPs) on how to identify and validate weaknesses/vulnerabilities on web applications and their supporting systems (infrastructure) to include servers, database servers, mainframes, and databases. SOPs included step by step procedures to be used during the test, not including research.
- Developed scripts to simplify testing of infrastructure/applications; scripts may include discovery and/or exploits.
- Utilized Metasploit where possible to exploit any vulnerabilities where an exploit does exist. Modified open source scripts when necessary to exploit vulnerabilities. Used manual test procedures to validate any vulnerabilities.
- Rooted Android mobile devices and utilize them for reconnaissance and discovery on networks, and some scanning.
- Performed static and dynamic application security on bank mobile applications while they are in development, testing, and in production.
- Oversaw the security engineering and implementation of the infrastructure supporting the Affordable Care Act (ACA) applications.
- Supported event log monitoring, vulnerability management, change management, penetration testing of different ACA releases, and audit plan testing. Supported the integration and configuration of Guardium, SiteMinder, JBoss, webMethods, Oracle, ArcSight, and Greenplum into ACA.

Internal Revenue Service (IRS) April 2007 – November 2012
Director/Associate Director/Senior Security Engineer/Penetration Tester/Source Code Analyst

- As a Senior Security Engineer and the Associate Director, Security Engineering, managed and performed security engineering and information security controls testing, to include security controls assessments, vulnerability assessments, and penetration tests on client network devices, Windows and UNIX/Linux servers, SQL Databases, Web Applications, mobile devices and mobile applications.
- Procured and supported the implementation of nCircle, Guardium, Ounce/AppScan Web, Ounce/AppScan Source.
- Performed security engineering, to include developing security requirements, overseeing implementation, but also performed source code analysis and penetration testing on over 200 information systems to include Customer Account Data Engine (CADE) and CADE2, Electronic Fraud Detection System (EFDS), Where's

My Refund, Filing Information Returns Electronically (FIRE), AMS, RRP, Computer Security Audit Trails (CSAT), and other IRS information systems.

- Regularly briefed customers and clients on program/project progress; conduct Security+ and CISSP training on-site.
- As the Associate Director, Cybersecurity Operations, safeguarded the confidentiality, integrity, and availability of IRS information systems and taxpayer data through security engineering requirements, 24x7x365 event log monitoring, continuous monitoring of vulnerabilities, delivering security awareness briefings, incident handling, and implementing enterprise solutions to include Major Applications (MA) and General Support Systems) that process, transmit, or store Personally Identifiable Information (PII) and/or Sensitive but Unclassified (SBU) data.

Anne Arundel Community College **January 2005 – January 2015**
Adjunct Faculty/Instructor

- Mentored, instructed, and provided students in-depth coverage of the current security risks and threats to an organization's data. Also served the needs of individuals seeking to pass the CompTIA Security+, Net+, Linux+, and CISSP certification exams.

KPMG, LLP **October 2004 – April 2007**
Information Security Services Consultant/Pen Tester/Team Lead/Senior IT Auditor

- Member of the Information Security Services (ISS) Team leading and providing Information Security and IT Audit support to the federal government and commercial entities throughout the United States using NIST and DIACAP.
- Successfully traveled to over 30 sites and assessed over 30,000 information systems through active vulnerability scanning and infrastructure penetration testing in a three-year period, to include exploiting over 400 of those systems.
- Led and performed Security Engineering reviews, Infrastructure and Application Vulnerability Assessments, Penetration Testing, C&A, Policy Review, DR/BCP, Risk Assessments, Ethical Penetration Testing, Wireless Reviews, IT General Controls, Security Controls Assessments, Applications (Oracle, MSSQL, SAP, Hyperion, Lawson, etc.) testing in support of FISMA and FISCAM audits.
- Utilized knowledge of OMB-A 130, Appendix III, and NIST guidelines, including 800-18, 800-26, 800-30, 800-31, 800-37, 800-53, 800-61, and DIACAP, to support the preparation and approval of System Security Plans (SSPs) or System Security Authorization Agreements (SSA&As); support POA&M management. Supported the development of Test of Design and Effectiveness on Apps.
- Hands on experience in installing, configuring, testing, and hardening operating systems and applications to include Resource Access Control Facility (RACF).

Other Experience and Professional Accomplishments
Northrop Grumman Mission Systems
NSA and DHS, 02/99 – 09/04 – Senior Systems and Network Security Engineer
Fuentez Systems Concepts, Inc.
DISA, 11/02 – 05/03 – Senior Systems and Network Engineer
Sterling Software
Office of Naval Intelligence, 06/98 – 02/99 – Software and Security Engineer
United States Navy
Naval Security Group Activity, 06/88 – 05/98 – Spanish Language Analyst/Jr. Sys. Admin

Matthew Lane

Function and Specialization
Subject Matter Expert

- Information Security & Architecture
- Risk Management/Assessment
- Privacy
- NIST, ISO Controls
- IT Technology

Clearance
Public Trust Level 6; Security Risk Level 6C (High Level Public Trust); Critical, Level 3 with Access Level 2 (Secret) under National Security Positions by the CMS

Representative Clients
City of New York
Centers for Medicare & Medicaid Services
Santee Cooper Power Company
Capital District Transportation Authority

Certification(s)
INFOSEC Assessment Methodology (IAM) – National Security Agency – 2002
Certified Information Systems Security Professional (CISSP) – 2013

Education

Background

Mr. Lane has advised JANUS clients for many years on secure IT architecture and improved strategies. He has conducted technical and network analyses, assessments, audits, and penetration tests for many commercial and government entities. Specializing in today's aspects of e-commerce infrastructure and development of quality application code, he has identified architectural issues and vulnerabilities in many websites and organizations and has recommended specific solutions to a wide variety of clients. As a former developer he has contributed to the development and security of biometric authentication systems. He has designed VPNs (Virtual Private Networks), anonymous Internet connectivity, and a database security wrapper. He is a former instructor of Advanced Software Engineering at Columbia University, where he graduated Cum Laude with a degree in Computer Science.

Experience

JANUS Software, Inc. (d/b/a JANUS Associates) **May 1998 – Present**
Subject Matter Expert

- Advised Transit Authority on security risks, weaknesses in architecture and environment.
- Completed many vulnerability/risk assessments for government and commercial clients.
- Managed and conducted penetration tests for large power companies in the Southeastern United States, Midwest, and in the Northeast.
- Assessed SCADA and Industrial Control Environments for a large water distribution client in Massachusetts.
- Performed security audit remediation for wide variety of JANUS clients.
- Assessed security of a Smart Grid and connected appliance test for a major appliance manufacturer.
- Architected and advised on topics dealing with improved security controls for JANUS clients.
- Completed network security reviews and new architecture for variety of payment card industry clients.
- Engaged as an independent security expert by Counsel in the TJX retail security breach class action litigation.
- Retained as court appointed security expert in the Heartland security breach class action litigation.
- Completed detailed technology reviews for large number of commercial clients (Oracle, DB2, MS AD environments, and proprietary DB structures).
- Completed multiple security reviews of major power company.

B.S., Cum Laude – Computer Science, Columbia University, New York, NY, May 1999

A.A.S., Computer Science, Norwalk Community Technical College, Norwalk, CT, 1996

Technical Skills

C++, Java, Visual Basic, Perl, LISP, SQL, HTML, Active Server Page (ASP), Common Gateway Interface Programming (CGI), FTP, Telnet, TCP/IP, Mandrake Linux, Yellow Dog Linux, Red Hat Linux, NTServer/Workstation, Windows 2000/2003/2008/2012 Server, Windows 2000/XP/7/8, Microsoft Distributed File System (DFS), Microsoft Active Directory (AD) Administration, Microsoft Exchange 5.0/5.5/6.0 (2003), Microsoft DNS Server 2.0, Microsoft DHCP Server, Microsoft Proxy Server, Microsoft IIS, Microsoft Active Server Pages, Microsoft Internet Security Accelerator (ISA), Microsoft SQL 7.0/8.0, Sendmail 8, Apache Web Server, 3 Tier Architecture, Flexes z390 Emulator, Avocent AV works, VMWare server/eSXI/vCenter, Checkpoint VPN-1/Firewall-1 Next Generation (NG), Network Associates Gauntlet, Network Associates Certificate Server/Public key server, CyberCop Scanner, Core Impact, AppScan, MetaSploit, Rapid7, Nmap, Sniffer Pro, SATAN, Qualys, DataPower Configuration, 3COM Netserver, Cisco routers, Digex CSU/DSU, CORBA, RMI, DCOM, Enterprise Java Beans, Service Oriented Architecture, Cloud Computing Audits (FedRAMP), MQ, Digital Performer, ProTools, MAX, Sample Cell, Galaxy Librarian, Security Certification and Authorization Package (SCAP)

- Documented system interconnectivity and technical controls for the M.D. Anderson Cancer Center (MDACC).
- Completed Business Impact Analysis for major hospital leading to disaster recovery improvements.
- Project Manager for multiple engagements with the City of New York Department of Information Technology and Telecommunications (DoITT). These projects involved data sharing between multiple city agencies.
- Project Manager for Payment Card Industry audits of multiple agencies in the Commonwealth of Massachusetts.
- Project Manager for development of Biometric authentication system. This includes knowledge of the Microsoft GINA and authentication package.
- Performed software security application tests and accreditations for major clients based on NIST controls and HIPAA needs.
- Performed security assessment of one of the first two federal cloud approved sites.
- Lectured on topic of security monitoring and auditing procedures.

Consulting

- Assisted defense attorneys in the TJX data breach and Heartland data breach during the remediation periods and class action suits.
- Provided e-Discovery Litigation support for multiple clients.
- Performed Payment Card Industry (PCI) Scans and Audits for multiple corporate clients.
- Identified security controls throughout the lifecycle of systems for the Integrated Justice Project (IJP) in the City of New York.
- Spoke on the topic of Security in the System Development Life Cycle (SDLC) in the City of New York.
- Designed and executed disaster recovery tabletop tests of the M.D. Anderson Disaster Recovery plan.
- Developed a statewide contingency plan for the State of Wisconsin.
- Performed multiple security assessments for State of Wyoming Department of Health.
- Completed .NET security and controls application code reviews for clients.
- Member of a team that built the Security Certification and Accreditation Package (SCAP) for the Federal Aviation Administration.
- Performed Certification and Accreditation (C&A) and Systems Test and Evaluation (ST&E) for the Centers for Medicare & Medicaid Services (CMS).
- Developed a risk management program and maintained the Modulo Risk Manager software solution for the State of South Carolina.
- Developed security and operational policies and procedures for the Centers for Medicare & Medicaid Services (CMS) and the State of Wisconsin.
- Performed Risk Assessments (RAs) and System Security Packages (SSPs) for the Centers for Medicare & Medicaid Services (CMS), the Federal Deposit Insurance Corporation (FDIC) and the Department of Interior (DOI).
- Identified threats and vulnerabilities for the Federal Deposit Insurance Corporation (FDIC).
- Performed security reviews on a prototype IBM Websphere/Webseal/Policy Editor Installation for the Social Security Administration (SSA). Worked closely with SSA engineers to enhance the overall security of the system and bring it to production.
- Designed and implemented database solution for large government project.

Documentation, NYC DoITT Accreditation Process and Procedures, NYC DataShare security assessments, OWASP based security assessments, Single Sign-On (SSO) development with J2EE, AJAX, Cognos, three tier architecture, testing multiple environments in the NYC DoITT environment (IJP/DataShare), Firewall Configuration, Wireless Security Analysis, Web Based Kiosk Security Configuration Review, Automated Source code and Manual Source code reviews, Software Engineer for BIO*GATE (a Biometric integration with Active Directory)

- Conducted many PCI related penetration tests and audits. Multiple Reports on Compliance (RoC) submitted and approved by Visa for both Level 1 Merchants and Service Providers.
- Designed a vulnerability tracking and reporting system for the Centers for Medicare & Medicaid Services (CMS), which allowed management to generate real-time reports on the status of system upgrades and security risks. This system has since been enhanced to automatically produce Plan of Action and Milestones (POA&M) reports.
- Assessed security controls protecting the Oregon State Lottery's revenue streams. These reviews included inspection of Novell, Windows NT, STRATUS and Windows 2000 servers.
- Completed components of Security Certification and Accreditation for the Federal Aviation Administration (FAA).
- Analyzed network traffic and modified routing/firewall procedures to meet security standards for multiple clients.

Software Development/Code Reviews

- Developed the Application Recovery and Continuity Package (ARCPac) used by JANUS to manage, assess and report on the status of application business resiliency across an enterprise. ARCPac was a Connecticut Quality Assurance Silver Medal Award for Excellence winner in 2003.
- Developed the Vulnerability Assessment and Corrective Action Plan (VaCap) system for the Centers for Medicare & Medicaid Services (CMS). VaCap allowed multiple security assessors to enter vulnerabilities, track the corrective actions, report on risk acceptance, and summarize risk levels to federal auditors.
- Helped develop BIO*GATE - a biometric authentication system for the Windows operating system. BIO*GATE facilitates multifactor authentication and multi-modal authentication across vendors. BIO*GATE leverages the Biometric API (BioAPI) to increase its portability and usability.
- Named on multiple patent applications for BIO*GATE.
- Designed and built load balancing tool for high-level federal judiciary. This tool also increased the level of anonymity of employees while using the Internet. (Judicial Entity)
- Conducted a code review for the Social Security Administration (SSA) designed to identify coding flaws that could result in system unavailability or compromise. This review focused on the CGI interfaces, but did include reviews of stored procedures in the OS/390 environment and access to the COBOL data structures used in these procedures.
- Recitation Instructor for Advanced Software Engineering at Columbia University (Spring 1999).

Information Technology Design/Support

- Implemented cloud/virtualized infrastructure.
- Trained junior security staff members on the topic of security monitoring, auditing procedures, coding, and system design and change control procedures.
- Architect of Local Area Network and manager of Web, Mail and DNS Servers. This includes experience with Windows NT 4.0/2000/2003/2008/2012, OS2, OS390, z390 Linux and AIX nodes.
- Architect of 3-Tier architecture and associated management network.
- Designed and implemented corporate Virtual Private Network (VPN) for multiple clients.
- Assisted clients to acquire new hardware and software.
- Provisioned multiple T1 connections, DSL connections, Fiber Connections.

- Worked with a development team on the production of large, graphically oriented reports.
- Trained staff in penetration testing techniques and application testing techniques.
- Developed security tools, solutions to evaluate various security elements within Windows NT environment.

Sales and Sales Support

- Participated in scoping activities for PCI Assessments.
- Participated in multiple sales presentations to clients.

CPI Consulting Associates **1994 – 1998**

Graphic Designer/Chief Programmer

- Developed CIMBal, a mathematical model of the global chemical industry and supporting help programs.
- Engineered server-side applications in Java for the World Wide Web.
- Developed multi-user applications in Visual Basic.
- Worked with a development team on the production of large, graphically oriented reports.
- Designed a custom Web-based Single Sign-On (SSO) application.

Other Experience and Professional Accomplishments

- Presented Webinar "Integrating Your Vulnerability Management Program into Your Change Control Process", December 2016
- Presented Webinar "Building a Cyber Security Roadmap on a Limited Budget while Understaffed", July 2016
- Presented "Securing your OmniChannel Environment" at the New York Retail Connections Show in June 2015
- Panel member, Cyber Security, Connecticut Technology Council, March 2015
- Presented "The Internet of Everything" at the New York State Cyber Security Forum, June 2014
- Presented "Cyber Warfare: The Reality is that we are all Under Attack" at ANDI Outsourcing Summit in Cartagena, Columbia, May 2014
- Cyber Security presentation at the Retail Connections 7th Annual Business Executive Summit in Houston, Texas, March 2014
- Presented "Cyber Warfare: The Reality is that we are all Under Attack" at the International Association of Outsourcing Professionals Annual Summit, Orlando, Florida, February 2014
- Keynote Speaker on "Cyber Warfare and Cyber Security" at the North Carolina Association of CPAs Winter Conference, December 2013
- Panelist on "The Cloud and Cloud Security" at the Connecticut Technology Council IT Summit, November 2013
- Presented "Cyber Warfare: The Reality Is that We Are All Under Attack" at the 16th Annual New York State Cyber Security Conference/8th Annual Symposium on Information Assurance, June 2013
- Presented "Cloud Infrastructure: Too Big To Fail" at the CMS Best Practices conference, Jacksonville, Florida, February 2012
- Presented "Securing the Private Cloud" at IT for Government 2011 in Dubai, UAE, October 2011
- Presented "DRBC - Did your plan work? Will it work?", December 2011
- Panelist on "Private Cloud Infrastructure", November 2011

	• Interviewed by WNPR on the topic of "Small Business Utilization of Private Clouds", November 2011 • Presented a Payment Card Industry (PCI) Data Security Standard (DSS) compliance seminar to the Commonwealth of Massachusetts e-Commerce program members, 2008 • Presented an Application Testing Methodology to the Department of Information Technology (DoIT), City of New York, 2007 • News 12 Connecticut: Video Interview, Discussion on virus outbreaks and worm infestations during the Code Red infestation, 2002 • Interviewed by National Public Radio with respect to the Anna Kournikova Worm, February 2001 • ECII Conference on Electronic Crime, October 2000. Panelist and Speaker on the topic of "The hazards of integrating Legacy Systems with web applications" • News 12 Connecticut: Discussion of the "Blaster" worm and description of its effects on network bandwidth • Interviewed on CBS News radio. Discussed the "I Love You" virus and social engineering with respect to hacking, May 2000 • Vanguard Conference, June 1999. Lectured on Security Auditing and Monitoring

Function and Specialization

Subject Matter Expert

- Information Security
- IT Implementation
- Risk Management
- FISMA Assessments
- Penetration Tests
- Security Assessments

Clearance

U.S. Federal Civilian Agency High Public Trust PT6

Representative Clients

Commonwealth of Massachusetts
New York State
Centers for Medicare & Medicaid Services

Certification(s)

Offensive Security Wireless Professional

Education

B.S., Computer Engineering, Boston University, 1995

Technical Training/Skills

C, C++, Java, JavaScript, PHP, XML, Python, Android Mobile Development, Visual Basic, Perl, PowerShell, SQL, HTML, Common Gateway Interface Programming (CGI), Oracle Databases, MySQL,

Adam Fisher

Background

Adam Fisher has over 18 years of technical experience in risk assessments, information security, Independent Verification and Validation, penetration testing, application reviews, and systems analysis for major JANUS clients. He has an extensive background in system-level requirements and application code issues and has performed application security code reviews for major government and corporate clients. He is also an expert in biometric and multi-factor authentication and security and designed all the security features into a commercial biometric product.

Experience

JANUS Software, Inc. (d/b/a JANUS Associates) **March 1999 – Present**
Subject Matter Expert

- Led IT re-architecture and re-organization for advanced manufacturing client.
- Performed application security code reviews for web facing applications for major U.S. insurance company.
- Performed HIPAA compliance and risk assessments for U.S. Centers for Medicare & Medicaid Services for several years.
- Performed an in-depth research product assessment for government agency for needed software solutions.
- Tested major federal data center for adequate controls over risk and implementation of security requirements.
- Performed multiple system security tests for a major national corporation.
- Performed operating system, network, and physical risk assessment for major private brokerage firm.
- Performed application security code reviews for large federal government agency sensitive programs.
- Performed risk assessment and penetration test for global telecom organization.
- Senior security and risk advisor for major smart grid devices for major manufacturer.
- Performed multiple external and internal penetration tests and vulnerability assessments for major JANUS clients.
- Designed and implemented information security controls for biometric security product.
- Worked with biometrics vendors to integrate their products in secure manner.
- Advised on security of biometric products to various vendors.
- Developed technical test protocols designed to test new applications for vulnerabilities.
- Co-lead on the design and development of a new cutting-edge security package.

Intel 80x86 Assembly, Pascal, Intel and Motorola micro-controllers, biometric devices (proprietary and BioAPI), Lab View, DOS, Windows 3.x/9x/NT/2x/XP/2K3/Vista/2K8/7/8/2K12, UNIX, Linux, Desktop Publishing, Computer Hardware Design, Network Design and Installation, FTP, Telnet, TCP/IP, Microsoft Active Directory (AD) Administration, Microsoft DNS Server 2.0, Microsoft DHCP Server, Microsoft IIS, Microsoft Active Server Pages, Microsoft Internet Security Accelerator (ISA), Microsoft SQL 7.0/8.0, Apache Web Server, VMWare ESXi

OWASP ZAP, Metasploit, Nessus, Rapid7, Nmap, Cisco routers, CORBA, RMI, DCOM, Enterprise Java Beans, Service Oriented Architecture. OWASP-based security assessments, Single Sign-On (SSO) development with three tier architecture, testing multiple environments, firewall configuration, wireless security analysis, web-based kiosk security configuration reviews, automated source code and manual source code reviews, biometric integration with active directory.

- Prepared security solutions for web-based security training modules for large government agency.

Project Management

- Project managed development of new software solution involving complex components and interoperability requirements.
- Developed system requirements for multiple project builds.
- Managed and performed software testing of new versions of software builds.
- Developed requirements for, researched available products, and oversaw implementation of COTS product software installer module.
- Developed and gave technical presentations to high-ranking officers at Fortune 500 Companies, government officials, and contractors.
- Piloted biometric security solution for U.S. Office of Secretary of Defense.
- Managed new technology logistics between sales, marketing and development.
- Maintained associations with product partners and future/current clients.
- Performed on-site biometric installation and support for numerous clients.

Raytheon **June 1995 – February 1999**
Engineer

- Created a DOS-based GUI in ANSI C to monitor real-time simulation variables in missile simulation data analysis.
- Software lead on a multi-million-dollar upgrade of outdated legacy computer system. Duties entailed system concept design and requirements.
- Using National Instruments LabView, designed a Graphical User Interface (GUI) for the testing, calibration and usage of multiple I/O ports on a UNIX based system for real-time usage.
- Designed and implemented a real-time GUI interface for monitoring of real-time missile simulation. Built the application in Visual C++ using Microsoft's MFC and OpenGL Graphics standard.

Other Experience and Professional Accomplishments

Volunteer at Boston Children's Museum Computer Clubhouse instructing inner-city children in computer technology.

Team Leader of a successful project group that designed and constructed a monitoring device for measuring the amount of deflection in a sailboat's mast. Duties included physical design of the main computer and assistance in programming of the micro-controller component.

OTHER RELEVANT MATERIAL

Management Plan

Information Technology security projects have been specialty areas of ours for over 30 years and we staff our engagements with experienced people who possess high caliber technical capability and also business savvy. Our teams include veterans from such well-known companies as Raytheon and IBM, and from the military, government, banking, and law enforcement. The staff combines experienced information security professionals with highly energetic, bright people who live, work and breathe the Internet and the secure connectivity needs of clients. This blended experience means clients receive the benefit of the newest skills, along with the wisdom of years of organizational experience. This blend allows us to understand that your security and control requirements must be considered within the context of, and be appropriate to, the education and regulatory environment in which you operate.

We adhere to a stringent policy of cross-training and skills improvement such that each employee can fulfill more than one consulting role while still meeting the "expert's expert" performance standards demanded. All our employees practice multi-tasking on a daily basis, continuing to build their expertise, within the organization, enabling them to transfer that capability to your needs.

In all situations, we work to pair excellent consultants with the specific needs of the client. With a wide variety of skills available and a number of specialists in this field, we are always able to select appropriate staffing. Detailed resumes are provided so that experience can be determined directly by the client.

The number of staff used in any particular assignment depends on the needs of the client, how quickly the work needs to be completed, and how much room is available for multiple staff when on-site, etc. We can accommodate any of these.

Our staff members hold a number of certifications. These vary since we sponsor our employees to hold different certifications that, together, bring a richness of capabilities to our clients. These include the National Security Agency (NSA) Information Assurance Methodology (IAM), CISSP, CISA, multiple Microsoft certifications, CGEIT, CISM, CRISC, CEH, CCSK, MBCI, etc. However, we do not depend solely on certifications. Some staff members are extremely talented individuals who hold no certifications and we would match their capabilities against any certified staff anywhere.

In addition to skill, ethics is a major component of our work. Our employees are bonded and undergo background checks (criminal and credit) prior to employment. We also carry Errors and Omissions insurance and Cyber Liability insurance as additional levels of protection for clients. Employees sign a five-page ethics code upon employment that defines their behavior and stresses that they are to put the needs of our clients first in all situations.

Project management begins with contact between our Project Manager (PM) and the equivalent at the City. From this initial, introductory meeting, you will gain a solid background in how we believe the process should unfold to best serve you. After discussion, together, we will finalize this.

Portal capability through a secure portal will be set up early in the project so that rapid communication of information can be effected. Uploads of deliverables are deposited with version control. This ensures that security of the City's information is maintained and provides an easy way for the City staff to quickly and securely receive results.

Periodic status meetings will be held to discuss progress, activities for the period, issues, deliverables completed, risks to the program, and other items that need to be addressed.

Project Management Approach

JANUS ensures the quality of our services by emphasizing that only performance of the highest caliber meets our standards. Nothing less is tolerated. JANUS' project managers employ industry recognized methodologies as defined by the Project Management Institute (PMI) when and where appropriate to ensure "sanity" to what are often hectic schedules and complicated tasks.

Project Planning

We are adept at guiding projects to successful completion and are prepared to begin this project within a mutually agreed-to schedule. Because we have conducted so many similar projects over so many years, we are adept at foreseeing potential delays and logistical complications, and will develop both project plans and schedules that anticipate the typical complications that might arise in any project.

Although our management process incorporates the following elements, these will be structured to be as efficient as possible to meet your needs:

- ✓ Scope and Cost Management
- ✓ Schedule Management
- ✓ Human Resources Management
- ✓ Communications Management
- ✓ Risk Management
- ✓ Quality Management

Each topic is discussed in detail below.

Scope and Cost Management

We will include in our planning:

- ✓ Regular scope alignments with you

- ✓ Establishing mechanisms that help facilitate identification of changes to our scope and analyzing their impacts
- ✓ Mechanisms for documenting scope changes and identifying the communications protocols for communicating and gaining approval for any scope change prior to executing work on any new task(s)

These all have an impact on cost. In addition to scope, schedule will be managed to ensure that we meet the due dates of the project, thus also affecting cost.

Schedule Management

JANUS always works from a detailed project plan in MS Project that provides the tasks timeline, and resources for our work on the project along with the City and third-party vendor dependencies. Within our planning we will establish protocols for schedule management including:

- ✓ Frequency of schedule updates
- ✓ Process for creating schedule updates including clear roles and responsibilities between our team, the City, and other applicable stakeholders
- ✓ Protocols for communication of schedule status or changes or approvals

Human Resources Management

Human Resources Management is critical to our ability to properly align the appropriate skill sets with project needs. This will be true for this project also where we will need to provide subject matter professionals with network, infrastructure, application, policy, governance, etc. experience. We will discuss these needs with you, as part of our planning, to include the following:

- ✓ Refinement of the organizational structure offered within this proposal based on input and feedback from you
- ✓ Clear definition of roles and responsibilities within the engagement in coordination with the scope and objectives section of the project
- ✓ How we will manage staff changes (if any)
- ✓ Mechanisms, including communication channels for you, for handling potential performance concerns

Communications Management

We believe that to be effective in our role, it will be important to define clear communications protocols to provide mechanisms to:

- ✓ Report status including establishing templates
- ✓ Communicate status of scope, schedule, progress, and budget
- ✓ Identify tools for project tracking

In this element, we will also manage education and training. Although not specifically requested, JANUS always welcomes our client's staff to work along-side our staff to better understand what we do. This knowledge transfer also includes our offer of briefings each day to help your personnel follow where we are in the testing, what we are discovering, and to allow them to ask questions to increase their knowledge.

Risk Management

It is important for our team to manage risk within the project itself. Examples of these risks might include the need to bring in subject matter professionals to support previously unknown specific project needs or adjust work plans and schedules in response to unforeseen challenges. As a result, we will manage possible risks of our work. The approach we use includes a six-step framework process of Plan, Identify, Analyze, Respond, Track, and Communicate. Our team will determine risks that will be reported on, through any interim reports. Our goal of risk reporting is to identify risks, and report on them prior to their conversion into issues.

A sample risk issues log is presented below:

<table>
<tr><td colspan="5"><b>Total Issues</b>
16</td></tr>
<tr><td colspan="4"><b>Open Issues</b>
13</td><td rowspan="2"><b>Closed Issues</b>
3</td></tr>
<tr><td>Critical
0</td><td>High
1</td><td>Moderate
3</td><td>Low
3</td></tr>
</table>

This summary is supported by details behind each of the issues (see below).

Third Party Response		
Status: Open	**Level of Risk:** Moderate	**Stakeholder:** (name)
Description: the [redacted] vendor is not responding to repeated requests for information deemed important to the project.		
Action(s): Escalated to [redacted] management.		

Quality Management

Quality is also part of our Project Management approach. As consultants to organizations with complex needs, we subscribe to the standards of true quality and we keep them foremost in our dealings with clients. We believe that quality and information security and control are closely aligned.

How do we avoid quality non-conformance and encourage its opposite, conformance?

Planning

Quality in the control planning process itself equates to results that are effective, efficient, and proportional to the risk involved, no more (to ensure cost effectiveness) and no less (to ensure compliance and adequacy).

Thorough planning and significant experience in the type of project the City is requesting helps to avoid the price of quality non-conformance that has been shown to add so significantly to costs. With the price of non-conformance for American business averaging 25%-30% of costs (reprocessing, reruns, unplanned service, etc.), this is a situation that is too expensive to continue. No better time exists to ensure quality than in the planning phase.

Review, Checking, and Audit

We stress in our daily work environments the precepts of review, checking, and audit, both for our clients and ourselves. However, prevention is of even more value. We constantly stress prevention, and we assist each other in reviewing and checking tasks geared towards prevention.

Input

We are proud to work in an environment where our employees are highly valued members of the team. Therefore, each individual has an opinion that is considered, not only management's opinion.

The result of this structure has been that all our employees feel they are free to speak up about potential problems before they become actual problems. No problem gets buried. The staff works hard and commits long hours to their projects. However, they each can clearly see the results of their involvement.

Secure Communication

This project will require sharing confidential information. JANUS avoids using email attachments whenever possible, especially when confidential reports are being shared. To that end, JANUS will establish a secure portal dedicated to this project. Only JANUS team members and duly designated the City staff will have access to the portal. The portal is protected by advanced encryption and access controls.

Status Meetings

The purpose of this periodic meeting is to report on tracked project schedules, project milestones, logistics, and any metrics associated with project progress. At a high-level, actual findings and observations from the assessment and analysis can also be shared during the meeting. To be respectful of people's time, we recommend that the meeting be attended by the core project team, with others invited as needed according to the phase of the project.

Past Performance

Contract Name: Network Security Audit

a. Customer Name: Schertz-Cibolo-Universal City Independent School District (SCUC ISD)

b. Contract/Purchase Order Number: Purchase Order#: 108640	**c. Contract Type:** Fixed	**d. Total Contract Value:** $81,300.00

e. Brief Description of Work Performed:

Schertz-Cibolo-Universal City Independent School District (SCUC ISD) is a highly rated, public school district headquartered in Schertz, Texas serving over 15,000 students, with eight elementary, three intermediate, two junior high, and three high schools, and a staff exceeding 1800 persons.

JANUS provided SCUC ISD with an external and internal security vulnerability assessment, and cybersecurity maturity analysis, with emphasis on security maturity and authoritative security frameworks. The scope of the assessment included the following:

- External vulnerability assessment from the perspective of an outside attacker seeking to breach the external Internet defenses.
- Internal vulnerability assessment from the perspective of an internal hacker with direct access to the main internal networks.
- Web application security assessment of two on-premise and five hosted web applications.
- Wireless vulnerability assessment from the perspective of an outside attacker seeking to breach the internal defenses.
- Physical site review to assess the physical and environmental security controls at the SCUC ISD primary data center.
- Social engineering exercise to assess SCUC ISD security awareness.
- Compliance review:
    - Family Educational Rights Act of 1996 (FERPA)
    - Children's Internet Protection Act (CIPA)
    - Children's Online Privacy Protection Act (COPPA)

Assessment results were aligned with common security standards and frameworks:

- Center for Internet Security Top 20 Security Controls
- National Institute of Standards and Technology (NIST) Special Publication 800-53: "Recommended Security Controls for Federal Information Systems and Organizations"
- Open Web Application Security Project (OWASP) Top 10 Web Application Security Risks
- Capability Maturity Model Integration (CMMI)

JANUS worked with SCUC ISD to produce written deliverables and presentations for a variety audiences, and communicating risks and remediation advice in both technical and executive level formats.

f. Period of Performance: April 26, 2018 – July 30, 2018	**g. Technical/Project Manager:** Karla Burkholder, Ed.D.	**h. Contract Officer:**

	Director of Technology Schertz-Cibolo-Universal City ISD 1060 Elbel Road Schertz, TX 78154 Phone: 940-367-6841 Email: kburkholder@scuc.txed.net	

Contract Name: DIT Security Assessment
a. Customer Name: North Carolina Department of Information Technology

b. Contract/Purchase Order Number: PO# NC10301141	c. Contract Type:	d. Total Contract Value:
	Fixed	$255,400.00

e. Brief Description of Work Performed:

JANUS performed an assessment of the State of North Carolina's security posture to provide a detailed identification of application, system and network vulnerabilities; gaps in IT security governance; assessment of patching methodologies; current network security capabilities and potential existing security incidents. The assessment was based on the NIST 800-53 moderate control criteria with one report completed for each of the 37 application areas in-scope. The specifics included:

1. Identification of application, system, and network vulnerabilities and assessment of patching methodologies and was limited to publicly accessible hosts residing in the DMZ or Transaction Zones (TZ) that provide shared hosting environments. This included underlying Network Management and Out-of-Band zones and segments that provided network communications and services to the publicly accessible hosts.
    a. Conducted vulnerability scanning and current patching methodology assessment for DIT hosts, and end points (desktops and laptops).
    b. Conducted penetration testing for publicly accessible systems when initial vulnerability scanning identified potential high impact vulnerabilities.
    c. When penetration testing gained access to a system, the testing assessed the ability of the attacker to leverage the system for access to additional systems and networks.
    d. Conducted web application testing based on the current OWASP Top 10 listing.
2. Performed a security assessment against a sample of websites that were part of a Software as a service (SaaS) deployment. A security report was completed for this.
3. Gaps in IT security governance – JANUS reviewed and made recommendations on the DIT incident management plan.
4. Current vulnerabilities – JANUS reviewed the current vulnerability and patching process with recommendations on best practices to better secure the State.
5. Assessed current network security capabilities and their ability to identify and potentially stop cyberattacks, data loss, and misuse of IT resources.
6. Developed System Security Plan template for agencies to be able to complete for their individual needs.
7. Development of security training curriculum and presentation of two-day class to senior level personnel of the State.

f. Period of Performance:	g. Technical/Project Manager:	h. Contract Officer:
	Chip Moore	N/A

November 14, 2016 – February 1, 2018	Chief Information Security Officer North Carolina Department of Information Technology 3700 Wake Forest Road Raleigh, NC 27609 Phone: 919-754-6300 Email: charles.moore@nc.gov	

Contract Name: Network Infrastructure Assessment and Services **a. Customer Name: Texas Tech University Health Sciences Center – Higher Education/Healthcare**		
b. Contract/Purchase Order Numbers: CON1594817 **RFP:** 739-69130071	**c. Contract Type:** Firm Fixed Price	**d. Total Contract Value:** $199,364.38 New project value $422,000.00

e. Brief Description of Work Performed:

The Texas Tech University Health Sciences Center, (TTUHSC) contracted JANUS, to perform an assessment of its existing network infrastructure. Based on the conclusions of that assessment, JANUS provided further design recommendations to optimize the performance of the existing environment. The goal of this assessment was to provide TTUHSC's IT management with a clear understanding of the design, architecture, and performance of its existing network to ensure it is capable of meeting current needs as well as future strategic goals. (JANUS' recommendations are always vendor agnostic.)

The assessment focuses on a review of network requirements and technical architecture, to include:

- Layer 2 analysis: How network traffic is directed to and from end points, in a way that enables sufficient bandwidth and latency to supply acceptable levels of service while also ensuring security from intrusion and resilience from network failures.
- Layer 3: how various segments of the network across multiple campuses connect into a larger topology that ensures resilient connectivity and security across the entire infrastructure.
- Network devices and technologies, including an assessment of the readiness of the existing inventory of devices to meet current and future demands.
- JANUS also assessed TTUHSC tools and procedures for monitoring network health, performing root cause analysis on network issues, and addresses or remediates network issues.

In performing this assessment, JANUS conducted interviews with management and operational staff representative of TTUHSC's IT organization, conducted interviews and on-site assessments, and reviewed network diagrams, system monitoring tools, and log data provided by TTUHSC. In addition, JANUS conducted a suite of network tests to supplement TTUHSC's documentation and to validate assertions made in interviews.

For this assessment, JANUS performed the following services:

- Reviewed existing network documentation
    - Layer 2/3 network maps and diagrams
    - Firewall design and existing security zones
- Reviewed critical external dependencies
    - Federated authentication
    - Provider dependencies

- Reviewed Internet Protocol (IP) considerations, both current requirements and strategic outlook for IPv4 and IPv6
- Reviewed load and bandwidth utilization, and protocol analysis
- Conducted interviews with staff and management within the office of the CIO, and technical managers in each operational area
- Performed network scans to validate findings and assertions
- Performed an on-site physical survey in Lubbock
- Reviewed configuration of network monitoring tools
- Reviewed vendor documentation for critical infrastructure devices
- Reviewed inventory/equipment refresh documentation compiled by Network Infrastructure team
- Reviewed history and response to network events

JANUS provided assessment results in a series of reports and in-person presentations, grouping observations into, but not limited to, the following categories:

- Governance
- Fault Tolerance
- Network Availability and Stability
- Change Control and Configuration Management
- Bandwidth Considerations
- Quality of Service (QoS) and Voice over IP (VoIP)
- Network Authentication and Access Control
- IPv4 and IPv6 Protocols
- Wireless
- Automation
- Physical Environment and Equipment Lifecycle
- IT Service Management
- Security

The assessment was concluded with executive presentations and an open conversation about the future strategic vision.

f. Period of Performance:	**g. Technical/Project Manager:**	**h. Contract Officer:**
August 2016 – October 2016 Second Project: April 2017 – Present	Vince Fell Chief Information Officer and VP for Information Technology Information Technology Division Texas Tech University Health Sciences Center Preston Smith Library, Suite 165 3601 4th Street, MS 7755 Lubbock, TX 79430-7755 Phone: 806-743-7013 Email: vince.fell@ttuhsc.edu	N/A

Contract Name: Pennsylvania OIT Security Assessment

a. Customer Name: Commonwealth of Pennsylvania Office of Information Technology, Enterprise Information Security

b. Contract/Purchase Order Numbers: IT - ITQ 4400004480 PO#s: 4300415165, 4300457866	**c. Contract Type:** Firm Fixed Price	**d. Total Contract Value:** $157,042.23

e. Brief Description of Work Performed:

The Commonwealth of Pennsylvania Office of Information Technology (OIT) provides hosting, datacenter services, and information security services for all state agencies in the Commonwealth.

JANUS has completed three projects for the Commonwealth over three years.
Project 1: Provided external penetration testing and vulnerability assessment for the entire range of Commonwealth Internet facing hosts for dozens of state agencies. Phases of the project included:

- Network and host discovery across the entire range of 65,535 possible IP addresses
- Vulnerability scan across more than 1000 active internet hosts
- Application discovery to identify more than 500 active Internet applications and web sites
- Application vulnerability scans across more than 32,000 web pages
- Penetration testing, verifying vulnerabilities and attempting exploits against the top ten most important web sites
- Wireless penetration testing for the primary physical locations
- Social engineering, attempting to bypass physical security at the datacenter

Risk assessment results were delivered in a summarized 90 page report, supported by extensive spreadsheets of technical details that enable the technical support staff to remediated vulnerabilities. JANUS completed this project with an executive level briefing to the Commonwealth CIO and CISO.

Project 2: In year two JANUS repeated the network discovery and web application testing across the same ranges as in year one, and provided analysis of trends in risk and remediation of those sites and applications.

JANUS then provided penetration testing against that year's more important web applications, verifying vulnerabilities and demonstrating attack vectors that place Commonwealth assets at risk.

JANUS performed a social engineering email phishing campaign against 78,000 Commonwealth employees. This test included establishing a web site that looks like a Commonwealth web site. JANUS sent emails to all employees, where the email appeared to come from a known Commonwealth source, requesting that they log onto the fake web site and entered their username and password. JANUS tracked the individuals who entered their passwords, and provided an analysis of the departments that are most at risk from social engineering attacks.

Project 3: In 2016 JANUS performed two projects. The Department of State (DOS) contracted JANUS to perform a security assessment, vulnerability scan, and penetration test of its web-facing voter registration applications and the Commonwealth County Network (CCN), to include local Citrix terminals. In addition to technical testing JANUS reviewed the internal architecture and used it to determine how the services interconnect, what the various operability functions are for each, how users are able to interact with the Citrix terminals, and vulnerabilities or risks that arise from that architectural approach.

Voter registration web applications were tested from September 14, 2016 to October 4, 2016 and the private CCN network was tested on-site between October 17, 2016 and October 19, 2016.

The scope of this assessment included six (6) externally facing web sites, a thin client and the private network of T1 lines used to connect in a spoke and hub configuration to the Department's election systems in Harrisburg (via a third party outsourced arrangement run out of a Virginia data center), to manage voter registration records. The Department presents a Citrix virtual terminal session that county staff use to interact with Department systems. Because each of the 47 counties have their own independently managed network, uniform assurance of network security across the entire system cannot rely solely on county network security. The Citrix/private network configuration must protect Department systems from any hacking or misconfiguration originating from one of the 47 entry points. Testing was focused on:

- External penetration testing of web applications; and
- CCN network architecture, the Citrix terminal, and its general support systems. General support systems included Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP) servers, Gateways, and other DOS information systems.

All assessments included, but were not limited to, tests for minimum technical security controls defined by authoritative security guidelines and frameworks, including the following:

- NIST Special Publication 800-53: "Recommended Security Controls for Federal Information Systems and Organizations"
- Open Web Application Security Project (OWASP) Top 10 Web Application Security Risks

The rules of engagement for this security assessment and penetration test were as follows:

- All work must be accomplished within the specified time period.
- JANUS will not authorize or execute any functional changes on client networks.
- Testing will be conducted during normal business hours.
- JANUS will provide source IP addresses from which testing will be conducted.
- The DOS will be notified of the start and end of each daily testing period.
- Testing will include automated and manual techniques.

Results from testing were shared with the PA DOS as they were discovered, in an ongoing and collaborative process that enabled DOS to address vulnerabilities as they were discovered. At the conclusion of all testing JANUS provided a final report listing all vulnerabilities and risks, in a prioritized ranking for remediation, along with detailed recommendations for remediation.

Assessment results were presented in written reports and in-person executive briefings to the CIO of the Commonwealth.

f. Period of Performance:	**g. Technical/Project Manager:**	**h. Contract Officer:**
May 8, 2014 – August 15, 2014	Erik Avakian, CISSP, CISA, CISM, CGCIO, ITIL v3	N/A

May 16, 2015 – July 8, 2015 Voter registration web applications September 14, 2016 – October 4, 2016 The private CCN network was tested on-site between October 17, 2016 and October 19, 2016	Chief Information Security Officer Governor's Office of Administration Enterprise Information Security Office 5 Technology Park, Suite 108 Harrisburg, PA 17110 Phone: 717-772-4240 Email: eavakian@pa.gov	

NEEDS FROM CITY STAFF

When a project is agreed to specific items are regularly needed with which to carry out the project. Sometimes, clients do not attend to these details until the project has already begun and in such situations, the amount of testing and assessment or consulting contemplated in the project cannot be undertaken. We want you to obtain the most for your expenditures. Therefore, although not difficult to produce, JANUS does have the following needs:

Access to System and Staff

- Adequate access to management and other key personnel for consultation and interviews. Very little of these people's time will be taken, but some contact will be necessary;
- Access to technical and system programming staff (if needed) during the length of the project (very little time needed);
- Access to staff who have been identified for interviews during the length of the project (usually one hour each); and
- Immediate access on a part-time basis to a security (or staff) liaison person providing interface capability to assist with questions (when needed), contact with appropriate staff, etc. (low level of support) and establishing schedules. This is typically less than one-fifth time unless the person wishes to shadow our team to increase knowledge.

Logical and Other Access (when required)

- IP addresses relevant to project;
- User IDs/passwords for applications/operating systems (if needed);
- Authority to access network components and operating systems (as needed);
- Relevant documentation such as policies and procedures (if needed); and
- Letter of Authorization to access and test systems (format provided by JANUS when needed for the assessment).

Office Space/Physical Needs (if on-site)

- Identification badges, or equivalent should be available on arrival (if needed);
- Telephone connectivity;

- Lockable cabinet for documentation; and
- Workspace in which to work when on-site.

ASSUMPTIONS

1. Timely access to all resources (system and personnel) required to complete tasks and any interviewing (provided by the City within three (3) business days). Lack of this will impact our ability to perform our duties and could impact contents, deliverables and schedule.
2. Commitment and support from management and project stakeholders. The City will designate a senior-level individual who will be authorized during the term of the project to act as the project's primary contact. This individual must have authority to make decisions about actions to be taken by JANUS on behalf of the City for the proposed services.
3. The City acknowledges and agrees that if any City responsibility as set forth in this proposal is not performed by the City then JANUS will be relieved of providing the affected JANUS services to the extent the City's nonperformance impacts JANUS' ability to provide the affected services.
4. Availability of appropriate City staff and resources so that deliverables can be submitted, reviewed and accepted within the required timeframe.
5. The City Project Manager will be responsible for evaluating the appropriateness of recommendations with respect to overall needs.
6. The City will provide JANUS personnel with remote VPN access or install a JANUS appliance to all required internal systems where appropriate as determined by the City and JANUS.
7. The JANUS team will provide observations and recommendations to City project management during this engagement. The City is solely responsible for determining what changes/improvements should be implemented.
8. JANUS assumes one (1) draft and one (1) final submission of each deliverable.
9. Specific IP addresses, URLs, credentials, and other information related to test targets will be provided a minimum of ten (10) days before scheduled testing.
10. Scans will be allowed to execute to completion, including overnight execution.
11. If we are unable to complete a scan requirement specified within this proposal within thirty (30) days following commencement of the scan due to the City's failure to meet its obligations, the scan will be considered completed.
12. JANUS will perform work during normal business hours. Off-hours scans may be scheduled with advance notice. More than one postponement in off-hours scanning may result in scope changes.
13. Our staff will be provided proper credentials and access to conduct scans and tests.
14. Any delays to staff access will result in delayed deliveries or less test time available.
15. Permission from any cloud provider(s) must be granted.
16. The City acknowledges that the ability of JANUS to provide the services in accordance with the proposal (including the agreed pricing and delivery models) are contingent upon the accuracy

and completeness of information, data, and applications provided by the City as well as the City's cooperation and timely performance of its obligations.

17. Any attacks; e.g., during a penetration test, that could potentially cause a system failure, be it at the system or application level, will only be performed in coordination with the City. If the usage of the attack has been deemed as required to provide necessary coverage and authorization is gained from the City technical contact, then the attack will be performed.

OTHER ITEMS

Security Measures

JANUS is highly concerned about our clients' data and always takes precautions in holding or transmitting data. We also provide a secure site for client documentation to avoid using the Internet or mail. We can deposit deliverables in this portal for secure delivery of results.

As specialists in security, networking, and recovery, we understand the need for protection of client materials. Client electronic materials are kept secured within an access controlled data center so that no client materials can be exposed to unauthorized users. Printed materials are in locked cabinets, not left in the open.

As experts in cyber security, each JANUS employee is much more attuned to security needs than is an average company's employees. No one needs to force our employees to change passwords (or for them to be robust). Our people use proximity card badges as a matter of course every day. We operate in a Windows 2008/2012 server environment with high levels of security implemented. New generation firewalls (that are regularly monitored and tested) prevent unauthorized outsiders from accessing files and appropriate access privileges prevent unauthorized insiders from the same. Electronic files where client data are stored are in a locked-down file structure in a secure data center with only those who have a need-to-know having access.

In addition, when at a client site all our consultants work with encrypted laptops. Where "flash sticks" are utilized, these are also encrypted. The latest patches are applied prior to the laptops leaving our offices. Typically, prior to leaving a client site, all client data are loaded into a protected repository through a secure portal and the laptop is sanitized. In this manner, client data are not subject to loss or theft. Although this is perhaps over and above requirements for vendors, we take our responsibility as a security company very seriously and understand that we have a requirement to protect your information.

All our employees have signed confidentiality agreements and ethics statements and have undergone background checks which we also take seriously and all client materials are stored in files based on "need-to-know" prior to access being allowed.

While transferring documentation and reports back and forth between clients and our infrastructure, we encourage use of our secure portal which will be established for the City for this specific task at the beginning of the project. Thus, documents can be quickly checked in or out with version control to ensure security and speed. Access to this portal is also established on a "need-to-know" basis.

Vendor Neutrality

JANUS is a vendor neutral consulting company. We take no revenue from vendors in our consulting engagements and we sell none of their hardware or software. As vendor neutral consultants to both large and small organizations with complex needs, we subscribe to a high standard of results focused only on you, our client, with experienced project management and quality and we keep these foremost in our dealings with clients.

Bonding and Background Check Procedures

JANUS carries a criminal theft and fraud bond for $5,000,000 as well as liability and umbrella coverage. Our employees are bonded and undergo background checks (criminal and credit) prior to employment. We also carry both Errors and Omissions and Cyber Liability insurance as additional levels of protection for clients. Employees sign a five-page ethics code upon entry to JANUS that defines their behavior and stresses that they are to put the needs of JANUS' clients first in all situations.

In addition to background checks, many of our employees have also undergone separate background checks by federal and/or state agencies and typically often either hold, or are in the process of receiving, clearances for working with critical and sensitive data.

Change Order Process

As part of our quality plan, we utilize a formal change management process for all changes considered to a project's scope, deliverables, timeline, and budget. The change process includes steps, responsibilities, change parameters or measurement criteria and deadlines to guide the review of proposed changes for potential impacts and appropriateness prior to acceptance. Ensuring well-structured change management processes is a basic element of quality performance. Changes usually affect delivery dates, resources and costs. As a result, they need to be agreed to by both the City and our management before application to the project to make sure that all entities understand what is expected of them. Major items to be addressed within the Change Order Process include change requirement, priority, impact (to project scope), budget, and schedule.

APPENDICES

Appendix A – Tools

JANUS uses a variety of commercial, shareware, and freeware tools to conduct our risk and security assessments. The following list of tools reflects a sampling of those programs that have received thorough review and are frequently used by our consultants. However, other tools and programs are being reviewed and evaluated at all times, and it is common for other tools to be used in support of client requirements. In particular, there are literally hundreds of tools that are vulnerability/issue specific (such as msadcs.pl for taking advantage of the Microsoft IIS msadcs vulnerability), and are not covered in this list. Appropriate tools will be selected as JANUS moves through the testing phases of the project to meet the needs of the specific potential vulnerability or exploit we are attempting.

JANUS' staff is encouraged to search out, develop, and introduce new tools to all testers. In this way, we maintain our expertise in the latest available toolsets while at the same time focusing our efforts on those tools that will be the most helpful, without subscribing to every tool available. However, in addition to those tools mentioned below, which are part of our toolbox, we have a tool available to address any problem that a tester may encounter. All tools used are tested in a laboratory environment and receive a thorough review prior to their use on a client site.

Network and Packet Capture, Access, Sniffers, and Analysis Tools

Cain & Abel – A tool used to conduct man-in-the-middle attacks such as ARP poisoning, SSL Spoofing, and Wireless attacks. The tool can also be used to capture the Windows SAM files and hashes locally and has the ability to use dictionary attacks, mutations, and brute force to crack password hashes. JANUS uses this tool to intercept sensitive traffic on local network segments in order to discover credentials, test wireless network strength, and crack passwords.

Netcat – An open-source utility nicknamed "the Swiss Army Knife of network tools." JANUS consultants use this tool to provide network connections for numerous attacks.

NetworkMiner – A tool used to analyze and break down packet streams and to reconstruct files. JANUS uses this tool to perform complex analysis on packets which may reveal sensitive information.

Wireshark – A tool that is used to examine and capture a very wide range of interfaces and packet types, including: ARP/RARP, BOOTP/DHCP, DNS, Ethernet, ICMP, IGMP, IP/TCP/UDP, IPX, LPR/LPD, OSPF, PPP, RIP, SMB, SNMP, Token Ring, AppleTalk, and many others. JANUS uses this tool to capture and analyze packets on a network segment.

Network Mapping Tools

Hping2 – This is a ping-based program that is used to send customized and arbitrary TCP and UDP pings to remote hosts and networks. This tool is used by JANUS to gather raw fingerprint data and to provide functions particularly useful for examining firewall rules.

Nmap – This tool supports ping scanning (determine which hosts are up), port scanning (determine what services the hosts are offering by using SYN, ACK, FIN, XMAS, NUL, and UDP scans), and TCP/IP fingerprinting (remote host operating system identification based on kernel-level packet-handling techniques). This is the primary tool used by JANUS for port mapping.

Sweeper – A tool developed by JANUS staff designed to scan a range of IP addresses and perform scripted functions such as NSlookup, ping, and port fuzzing. JANUS uses this tool to assist clients in generating network maps and inventories.

Password Crackers

HashCat – A command line tool for cracking password hashes. This tool can crack dozens of different types of hashes based on various cryptographic standards. JANUS uses this tool to test hashes against dictionary files to find passwords.

HashID – A tool used to identify various hashtypes in order to identify the proper method for decryption. JANUS uses this tool to identify unknown hash values prior to decryption with other tools.

John the Ripper – A tool used to decrypt discovered password hashes using brute force and dictionary files. JANUS uses this tool to decrypt hashes to uncover usernames and passwords.

L0phtCrack – A tool used to decrypt password hashes and to crack a dumped SAM file, the registry, or sniffed SMB packets containing both LANMAN and NT hashes. JANUS uses this tool to decrypt hashes to uncover usernames and passwords.

Mutagen – A tool developed by JANUS staff to build custom dictionary files with over 500,000 mutations. JANUS uses this to create custom dictionaries for each engagement based on key acronyms, phrases, and non-dictionary words related to the client.

WCE (Windows Credentials Editor) – This tool allows users to: Perform Pass-the-Hash on Windows; 'Steal' NTLM credentials from memory; 'Steal' Kerberos Tickets from Windows machines; use the 'stolen' Kerberos Tickets on other Windows or UNIX machines to gain access to systems and services; and dump cleartext passwords stored by Windows authentication packages. JANUS uses this tool to gain credentials and assess the security of Windows networks.

System Tools

Harvester – This is a tool that is used to search for email addresses based on a domain name. JANUS uses this tool to search for possible targets and usernames for attacks.

I.C.U...MVS – A tool developed by JANUS staff to conduct audits and testing of mainframe systems. This tool is currently licensed to several federal agencies. JANUS uses this tool when conducting tests that involve mainframe systems.

Kali Linux – The most advanced and versatile penetration testing operating system. This operating system comes preinstalled with a variety of testing tools that can be used for assessments and penetration testing. JANUS uses this for access to multiple tools and applications not available through Windows.

Loki – A tool developed by JANUS staff to encrypt and decrypt strings based on known algorithms. JANUS uses this tool to decode cookies and to crack encrypted messages.

RAT – A tool used to assess Cisco Internetwork Operating System (IOS) and Cisco Private Internet Exchange (PIX) firewalls. JANUS uses this tool to assist with auditing Cisco devices.

SQLMap – This is a tool for automated SQL injections. JANUS testers use this tool to assist in testing SQL based applications for input validation vulnerabilities.

SiteDigger – A tool that searches Google's cache to look for vulnerabilities, errors, configuration issues, proprietary information and interesting security nuggets on websites. JANUS uses this tool to help automated searches for open source intelligence.

Vulnerability Scanners

Metasploit – This framework is an infinitely versatile application that enables automated exploits of vulnerabilities in order to gain access to systems. This framework is equipped with tools that cover the entire range of testing methodology from information gathering to post exploitation. JANUS uses this tool to discover systems, identify vulnerabilities, exploit known vulnerabilities, and perform post exploitation tasks.

Nessus – This application offers a variety of scanners and modules for many different device types and can conduct vulnerability scanning as well as network discovery, offline auditing, and file discovery. This tool is customizable and has been modified with custom checks by JANUS. This premier open-source vulnerability assessment tool is the primary vulnerability scanner used by JANUS for both penetration testing and vulnerability assessment.

Web Server/Web Application Tools

BurpSuite – This tool is a web proxy that captures and replays HTTP packets with permuted input. JANUS uses this tool to intercept and modify packets to identify hidden fields, capture sensitive information, and identify sessions.

Cookie Digger – A tool used to collect and analyze cookie values used to maintain session state and isolation through identifying the use of easily guessed or predictable cookie values. JANUS uses this tool to perform session hijacking in web applications.

Curl – This is an open-source network tool for retrieving files from the Internet using HTTP, HTTPS, and FTP protocols. JANUS uses this tool to access, download, and upload files to vulnerable web pages.

Firebug – This tool allows for close inspection of HTML and JavaScript in web pages and can edit local components. JANUS uses this tool to assist with manual analysis of websites for information and vulnerabilities.

GNU Wget – This is an open-source network tool for retrieving files from the Internet using HTTP, HTTPS, and FTP protocols. JANUS uses this tool to access, download, and upload files to vulnerable web pages.

httprint – A web server fingerprinting tool. JANUS uses this to identify the operating system and web server type of target systems.

HTTrack – This is an open-source off-line browser utility that downloads websites so that aspects can be manipulated and tested locally. JANUS uses this to copy pages for testing components and for social engineering.

Nikto – An open-source, command-line, web server scanner. JANUS uses this tool for both penetration testing and vulnerability assessments.

OpenSSL – This is an open-source library that provides cryptographic functionality to applications such as secure web servers. JANUS uses this application to create and distribute certificates used for spoofing.

OWASP Zap – The Zed Attack Proxy (ZAP) is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications. JANUS testers use this tool for both penetration testing and vulnerability assessments.

Qualys SSL Lab – This is an online tool for assessing the strength of a websites SSL certificates. JANUS uses this tool to test for vulnerabilities in the cryptography of web applications.

SEE – A tool developed by JANUS staff to host malicious web pages, generate malicious emails, capture credentials, and track usage for social engineering campaigns. This is the primary tool JANUS uses to conduct large social engineering campaigns.

SSLDigger – Provides a Graphical User Interface (GUI) to a tool used to assess the strength of SSL servers by testing the supported cipher. JANUS uses this tool to test for vulnerabilities in the cryptography of a web application.

Tamper Data – A tool for capturing and modifying HTTP/HTTPS headers in transit. A tool JANUS utilizes to further inspect sites for session information and vulnerabilities.

w3af – Web Application Attack and Audit Framework's goal is to create a framework to help secure web applications by finding and exploiting all web application vulnerabilities. This tool provides an automated framework for finding vulnerabilities in web applications. JANUS uses this tool for both penetration testing and vulnerability assessments.

Wireless Testing

Network Stumbler – This tool detects and identifies all wireless access points within range including those that do not broadcast their SSID. JANUS uses this tool to identify potential targets when mapping wireless networks.

WirelessMon – This tool detects and identifies all wireless access points within range including those that do not broadcast their SSID. This tool can also be paired with a GPS device to physically map the location and boundaries of the wireless area. JANUS uses this tool to map and identify the ranges of wireless networks for testing.

Kismet – This tool detects and identifies all wireless access points within range including those that do not broadcast their SSID. JANUS uses this tool to identify potential targets when mapping wireless networks.

Wellenreiter – This tool detects and identifies all wireless access points within range including those that do not broadcast their SSID. JANUS uses this tool to identify potential targets when mapping wireless networks.

WaveStumbler – This tool detects and identifies all wireless access points within range including those that do not broadcast their SSID. JANUS uses this tool to identify potential targets when mapping wireless networks.

AirSnort – This tool performs network discovery for wireless devices but also captures packets to perform man-in-the-middle attacks in order to recover/crack WEP encryption keys. JANUS uses this tool to break into secure wireless networks.

AirCrack – This tool performs network discovery for wireless devices but also captures packets to perform man-in-the-middle attacks in order to recover/crack WEP encryption keys. JANUS uses this tool to break into secure wireless networks.

OWASP

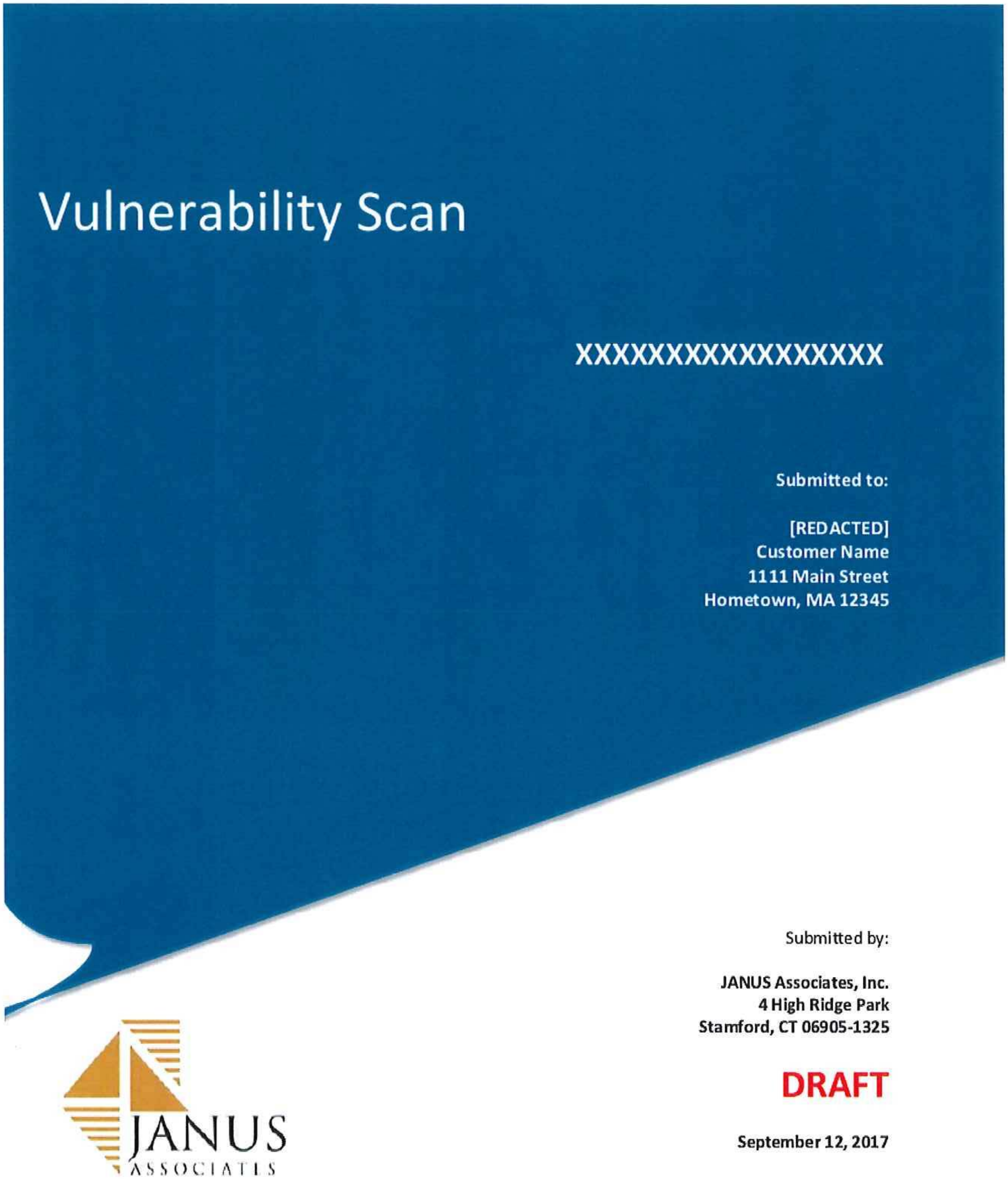
We also focus on the Open Web Application Security Project (OWASP) "Top Ten" in our assessments. To perform testing in this area we regularly utilize a variety of the following tools:

Attack	Tool
• Un-validated Input	SPI Dynamics Code Review tools
• Broken Access Control	SPI Dynamics Code Review tools
• Broken Authentication and Session Management	SPI Dynamics Code Review tools
• Cross-Site Scripting (XSS) Flaws	Web Inspect
• Protocol Analysis	Wireshark
• Buffer Overflows	Core Impact
• Injection Flaws	SPI Dynamics Code Review tools
• Improper Error Handling	Web Inspect
• Insecure Storage	ISS Database scanner
• Insecure Configuration Management	Alteris, SMS
• Physical Intrusion	Lenal OnGuard
• IP half-scan	MS ISA Server
• Brute Force Password cracking and access violation	LC4
• Cisco devices with SNMP	Foundstone tools
• Trojan horses	Symantec Corporate Edition 10.2
• Java-based DB analysis	NGS Squirrel
• Interceptions; most frequently associated with TCP/IP stealing and interceptions that often employ additional mechanisms to compromise operation of attacked systems (man-in-the-middle attacks)	HP OpenView
• Spoofing (deliberately misleading by impersonating or masquerading the host identity by placing forged data in the cache of the named server i.e. DNS spoofing)	ARPSpoof
• Scanning ports and services, including ICMP scanning (Ping), UDP, TCP Stealth Scanning (TCP that takes advantage of a partial TCP connection establishment protocol)	MS ISA Server
• Remote OS Fingerprinting, for example by testing typical responses on specific packets, addresses of open ports, standard application responses (banner checks), IP stack parameters etc.	NESSUS, Nmap

• Network packet listening (a passive attack that is difficult to detect but sometimes possible)	CISCO Monitoring tools
• Authority abuse; a kind of internal attack, for example, suspicious access of authorized users having odd attributes (at unexpected times, coming from unexpected addresses)	Windows Audit logs
• Flooding (Ping flood, mail flood, HTTP flood)	ARPSpoof, Nmap
• Malformed URL's	Apache mod_proxy
• Wireless Connection Attempts	AIRTight

Appendix B – Sample Reports

Vulnerability Scanning



Vulnerability Scan

XXXXXXXXXXXXXXXXX

Submitted to:

[REDACTED]
Customer Name
1111 Main Street
Hometown, MA 12345

Submitted by:

JANUS Associates, Inc.
4 High Ridge Park
Stamford, CT 06905-1325

JANUS
ASSOCIATES

DRAFT

September 12, 2017

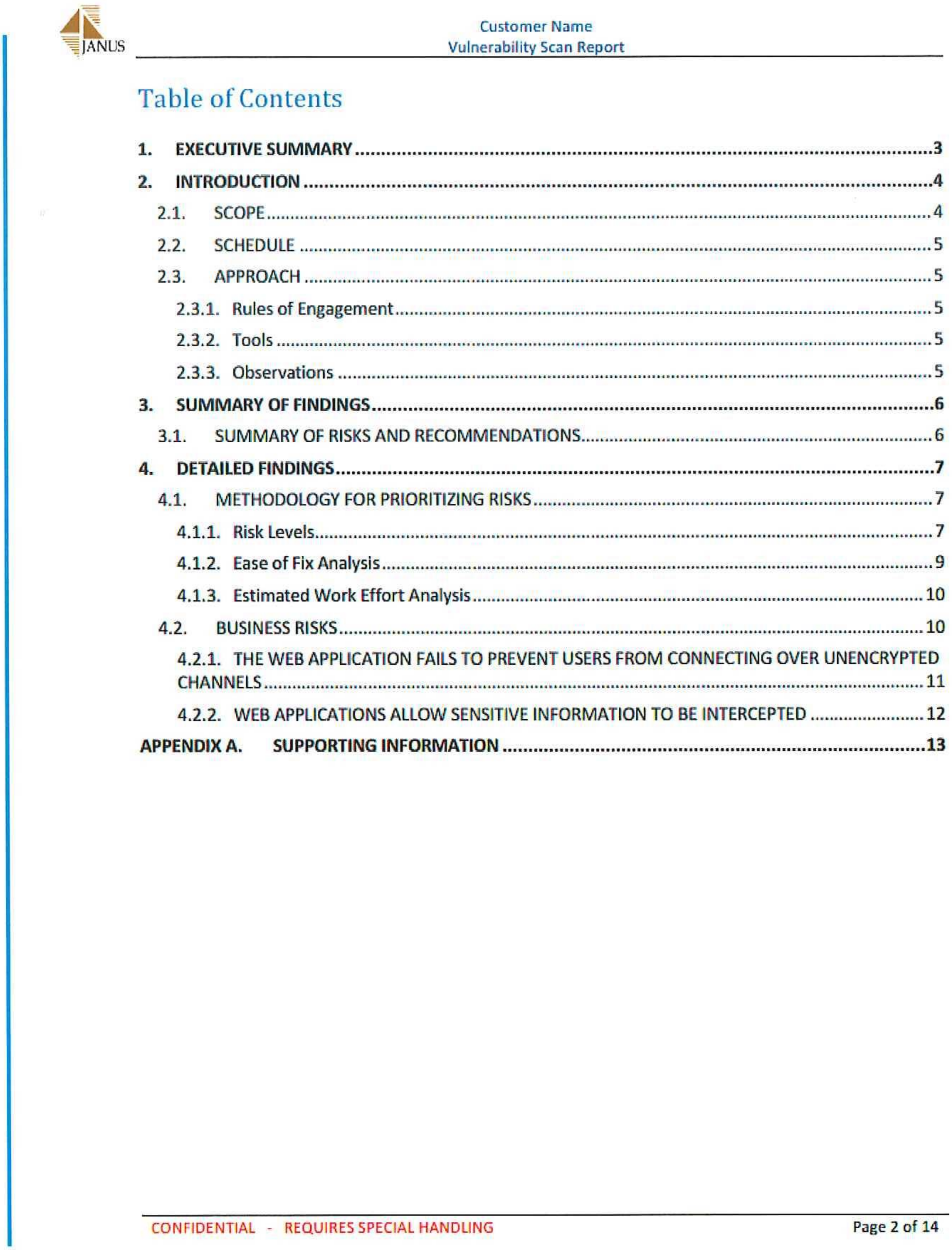
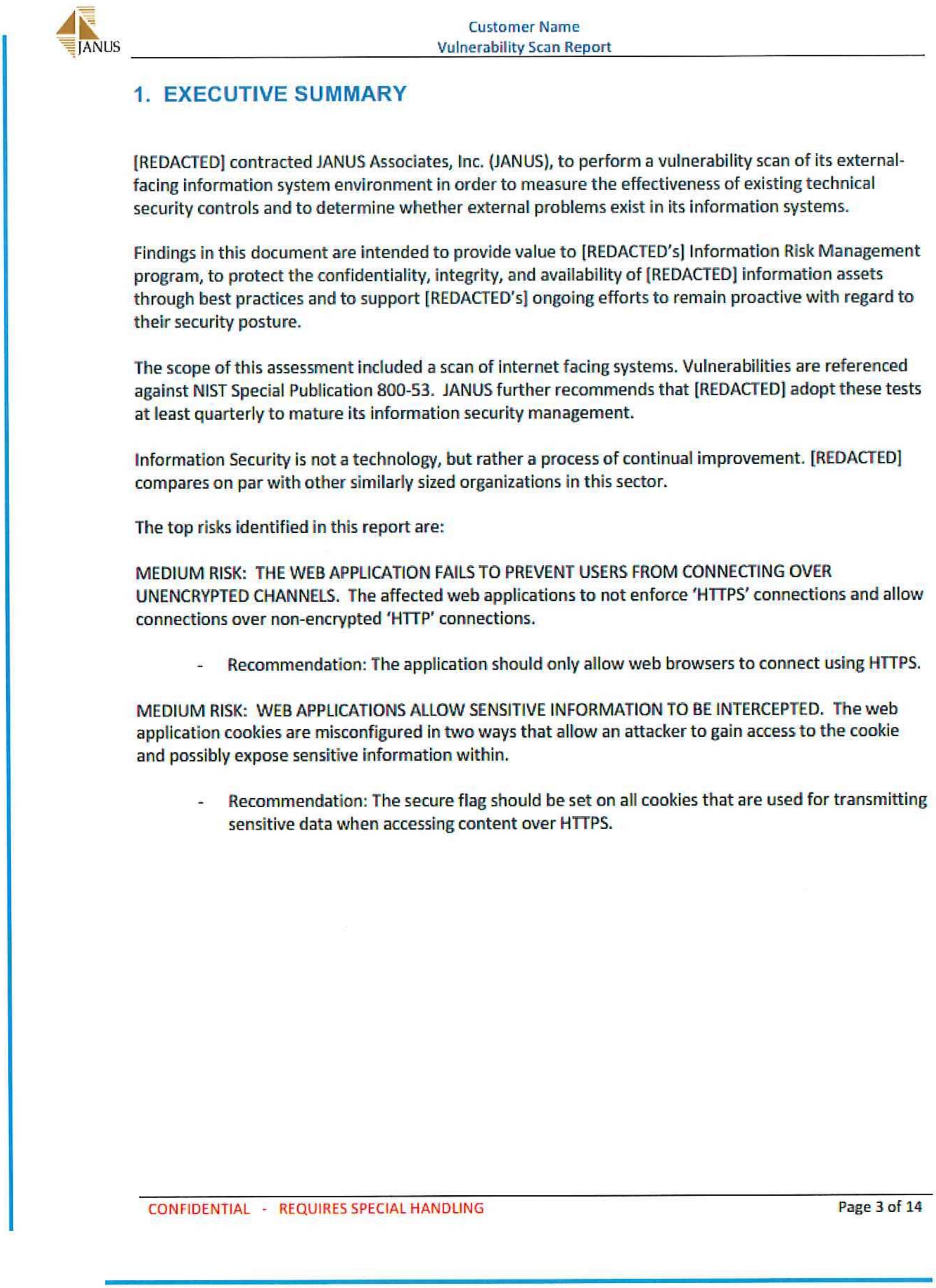


Table of Contents



JANUS

Customer Name
Vulnerability Scan Report

1. EXECUTIVE SUMMARY

[REDACTED] contracted JANUS Associates, Inc. (JANUS), to perform a vulnerability scan of its external-facing information system environment in order to measure the effectiveness of existing technical security controls and to determine whether external problems exist in its information systems.

Findings in this document are intended to provide value to [REDACTED's] Information Risk Management program, to protect the confidentiality, integrity, and availability of [REDACTED] information assets through best practices and to support [REDACTED's] ongoing efforts to remain proactive with regard to their security posture.

The scope of this assessment included a scan of internet facing systems. Vulnerabilities are referenced against NIST Special Publication 800-53. JANUS further recommends that [REDACTED] adopt these tests at least quarterly to mature its information security management.

Information Security is not a technology, but rather a process of continual improvement. [REDACTED] compares on par with other similarly sized organizations in this sector.

The top risks identified in this report are:

MEDIUM RISK: THE WEB APPLICATION FAILS TO PREVENT USERS FROM CONNECTING OVER UNENCRYPTED CHANNELS. The affected web applications to not enforce 'HTTPS' connections and allow connections over non-encrypted 'HTTP' connections.

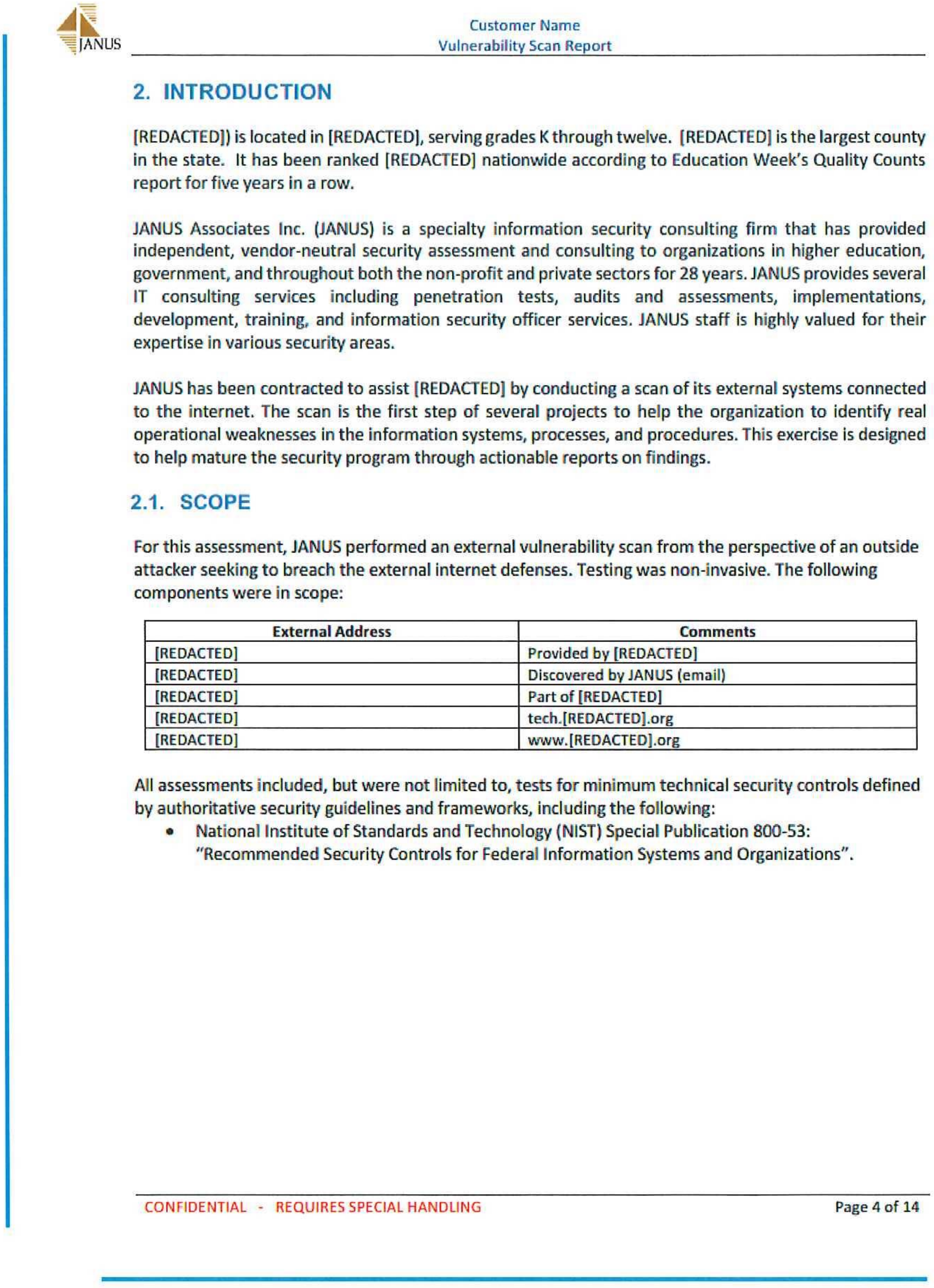
- Recommendation: The application should only allow web browsers to connect using HTTPS.

MEDIUM RISK: WEB APPLICATIONS ALLOW SENSITIVE INFORMATION TO BE INTERCEPTED. The web application cookies are misconfigured in two ways that allow an attacker to gain access to the cookie and possibly expose sensitive information within.

- Recommendation: The secure flag should be set on all cookies that are used for transmitting sensitive data when accessing content over HTTPS.

CONFIDENTIAL - REQUIRES SPECIAL HANDLING

Page 3 of 14



2. INTRODUCTION

[REDACTED]) is located in [REDACTED], serving grades K through twelve. [REDACTED] is the largest county in the state. It has been ranked [REDACTED] nationwide according to Education Week's Quality Counts report for five years in a row.

JANUS Associates Inc. (JANUS) is a specialty information security consulting firm that has provided independent, vendor-neutral security assessment and consulting to organizations in higher education, government, and throughout both the non-profit and private sectors for 28 years. JANUS provides several IT consulting services including penetration tests, audits and assessments, implementations, development, training, and information security officer services. JANUS staff is highly valued for their expertise in various security areas.

JANUS has been contracted to assist [REDACTED] by conducting a scan of its external systems connected to the internet. The scan is the first step of several projects to help the organization to identify real operational weaknesses in the information systems, processes, and procedures. This exercise is designed to help mature the security program through actionable reports on findings.

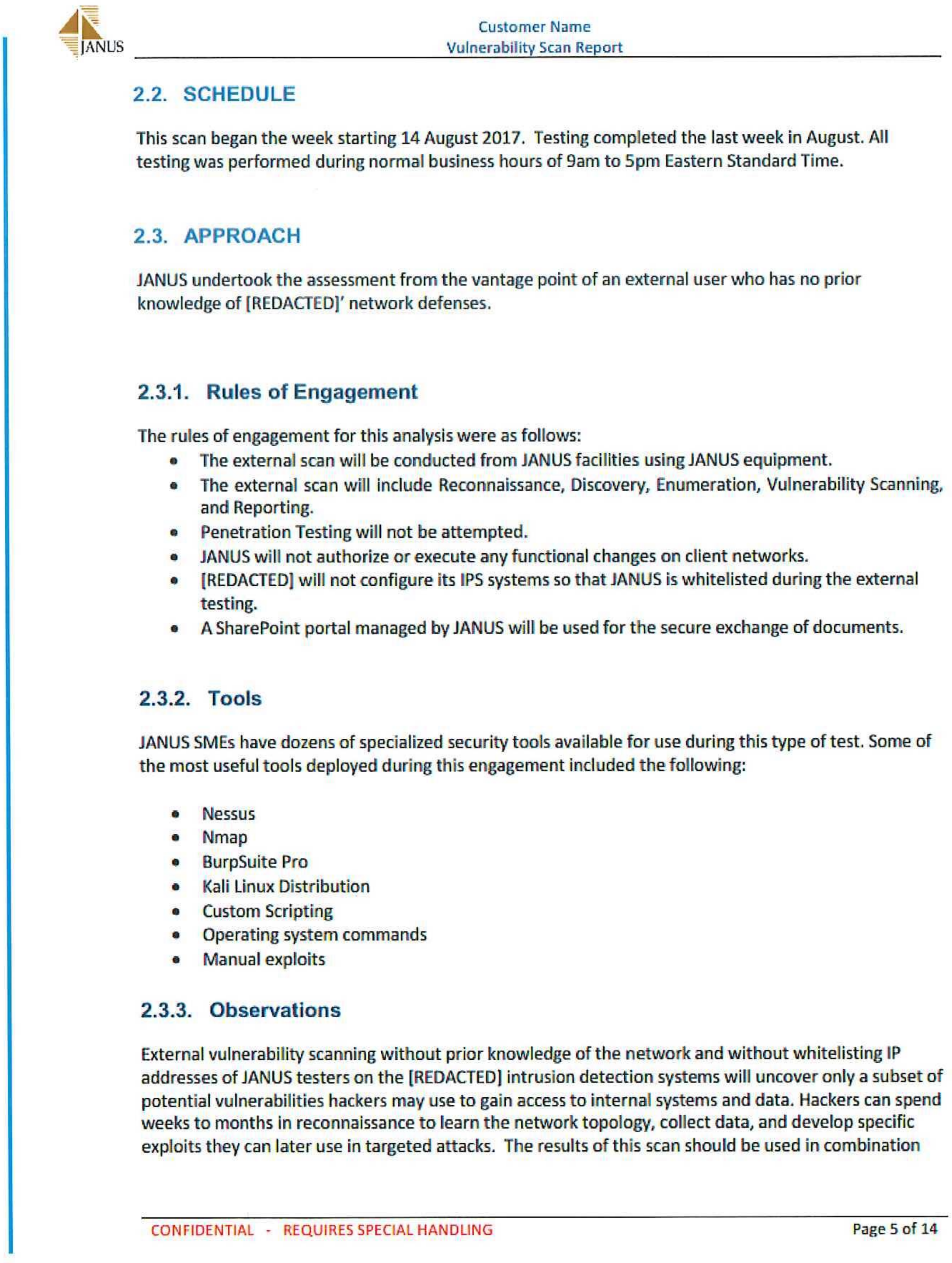
2.1. SCOPE

For this assessment, JANUS performed an external vulnerability scan from the perspective of an outside attacker seeking to breach the external internet defenses. Testing was non-invasive. The following components were in scope:

External Address	Comments
[REDACTED]	Provided by [REDACTED]
[REDACTED]	Discovered by JANUS (email)
[REDACTED]	Part of [REDACTED]
[REDACTED]	tech.[REDACTED].org
[REDACTED]	www.[REDACTED].org

All assessments included, but were not limited to, tests for minimum technical security controls defined by authoritative security guidelines and frameworks, including the following:

- National Institute of Standards and Technology (NIST) Special Publication 800-53: "Recommended Security Controls for Federal Information Systems and Organizations".



2.2. SCHEDULE

This scan began the week starting 14 August 2017. Testing completed the last week in August. All testing was performed during normal business hours of 9am to 5pm Eastern Standard Time.

2.3. APPROACH

JANUS undertook the assessment from the vantage point of an external user who has no prior knowledge of [REDACTED]' network defenses.

2.3.1. Rules of Engagement

The rules of engagement for this analysis were as follows:

- The external scan will be conducted from JANUS facilities using JANUS equipment.
- The external scan will include Reconnaissance, Discovery, Enumeration, Vulnerability Scanning, and Reporting.
- Penetration Testing will not be attempted.
- JANUS will not authorize or execute any functional changes on client networks.
- [REDACTED] will not configure its IPS systems so that JANUS is whitelisted during the external testing.
- A SharePoint portal managed by JANUS will be used for the secure exchange of documents.

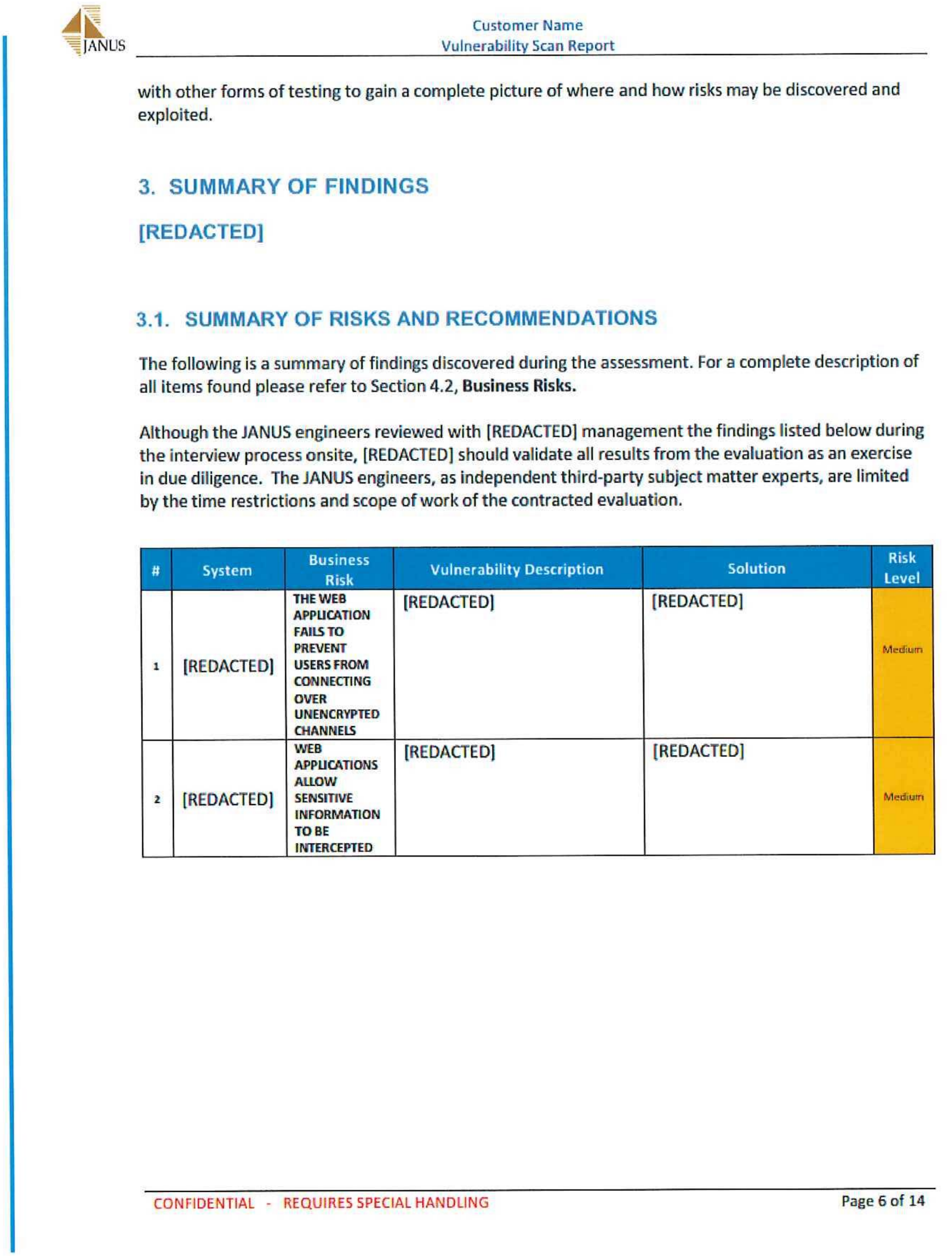
2.3.2. Tools

JANUS SMEs have dozens of specialized security tools available for use during this type of test. Some of the most useful tools deployed during this engagement included the following:

- Nessus
- Nmap
- BurpSuite Pro
- Kali Linux Distribution
- Custom Scripting
- Operating system commands
- Manual exploits

2.3.3. Observations

External vulnerability scanning without prior knowledge of the network and without whitelisting IP addresses of JANUS testers on the [REDACTED] intrusion detection systems will uncover only a subset of potential vulnerabilities hackers may use to gain access to internal systems and data. Hackers can spend weeks to months in reconnaissance to learn the network topology, collect data, and develop specific exploits they can later use in targeted attacks. The results of this scan should be used in combination



with other forms of testing to gain a complete picture of where and how risks may be discovered and exploited.

3. SUMMARY OF FINDINGS

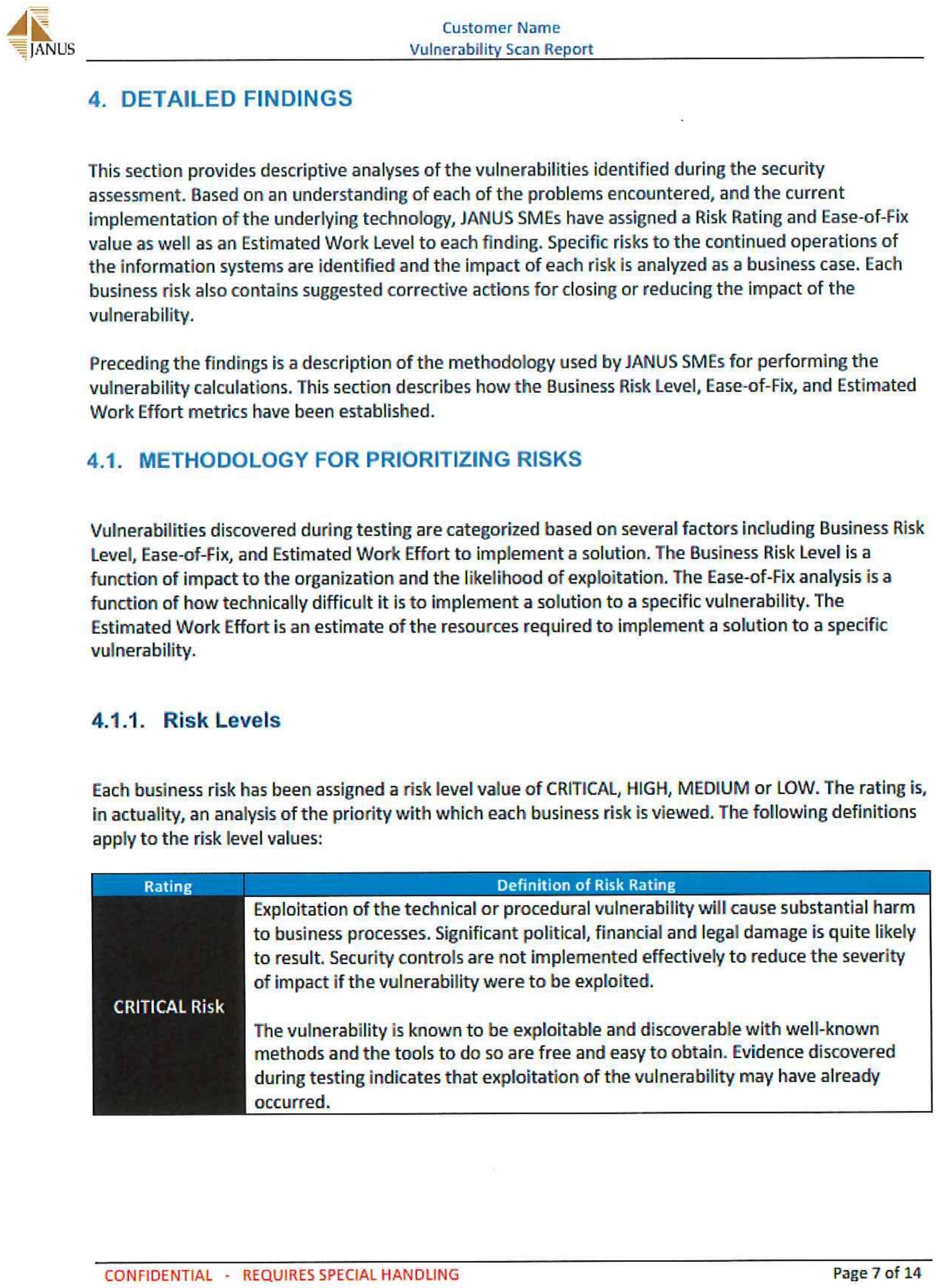
[REDACTED]

3.1. SUMMARY OF RISKS AND RECOMMENDATIONS

The following is a summary of findings discovered during the assessment. For a complete description of all items found please refer to Section 4.2, **Business Risks.**

Although the JANUS engineers reviewed with [REDACTED] management the findings listed below during the interview process onsite, [REDACTED] should validate all results from the evaluation as an exercise in due diligence. The JANUS engineers, as independent third-party subject matter experts, are limited by the time restrictions and scope of work of the contracted evaluation.

#	System	Business Risk	Vulnerability Description	Solution	Risk Level
1	[REDACTED]	**THE WEB APPLICATION FAILS TO PREVENT USERS FROM CONNECTING OVER UNENCRYPTED CHANNELS**	[REDACTED]	[REDACTED]	Medium
2	[REDACTED]	**WEB APPLICATIONS ALLOW SENSITIVE INFORMATION TO BE INTERCEPTED**	[REDACTED]	[REDACTED]	Medium



4. DETAILED FINDINGS

This section provides descriptive analyses of the vulnerabilities identified during the security assessment. Based on an understanding of each of the problems encountered, and the current implementation of the underlying technology, JANUS SMEs have assigned a Risk Rating and Ease-of-Fix value as well as an Estimated Work Level to each finding. Specific risks to the continued operations of the information systems are identified and the impact of each risk is analyzed as a business case. Each business risk also contains suggested corrective actions for closing or reducing the impact of the vulnerability.

Preceding the findings is a description of the methodology used by JANUS SMEs for performing the vulnerability calculations. This section describes how the Business Risk Level, Ease-of-Fix, and Estimated Work Effort metrics have been established.

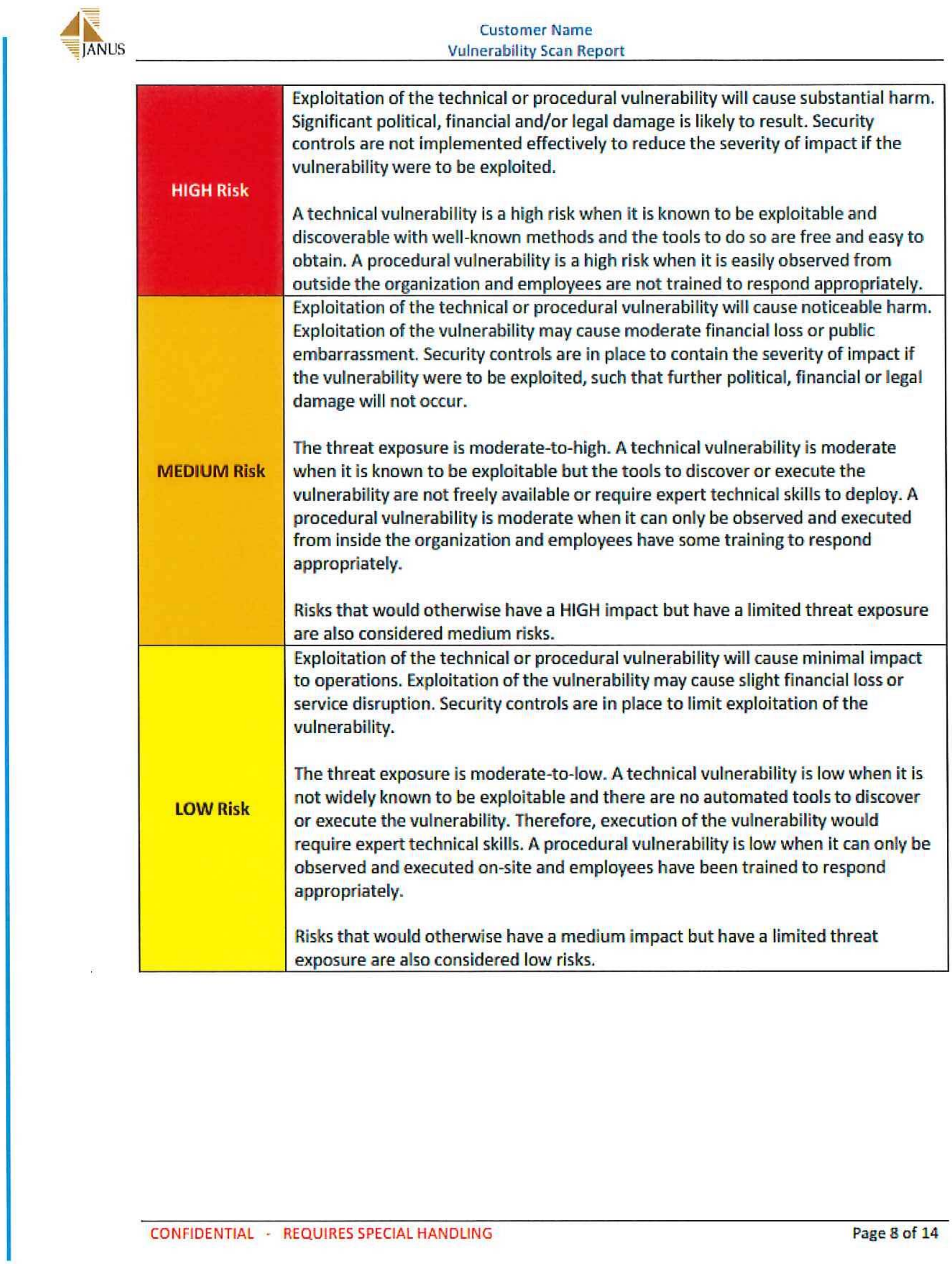
4.1. METHODOLOGY FOR PRIORITIZING RISKS

Vulnerabilities discovered during testing are categorized based on several factors including Business Risk Level, Ease-of-Fix, and Estimated Work Effort to implement a solution. The Business Risk Level is a function of impact to the organization and the likelihood of exploitation. The Ease-of-Fix analysis is a function of how technically difficult it is to implement a solution to a specific vulnerability. The Estimated Work Effort is an estimate of the resources required to implement a solution to a specific vulnerability.

4.1.1. Risk Levels

Each business risk has been assigned a risk level value of CRITICAL, HIGH, MEDIUM or LOW. The rating is, in actuality, an analysis of the priority with which each business risk is viewed. The following definitions apply to the risk level values:

Rating	Definition of Risk Rating
CRITICAL Risk	Exploitation of the technical or procedural vulnerability will cause substantial harm to business processes. Significant political, financial and legal damage is quite likely to result. Security controls are not implemented effectively to reduce the severity of impact if the vulnerability were to be exploited. The vulnerability is known to be exploitable and discoverable with well-known methods and the tools to do so are free and easy to obtain. Evidence discovered during testing indicates that exploitation of the vulnerability may have already occurred.



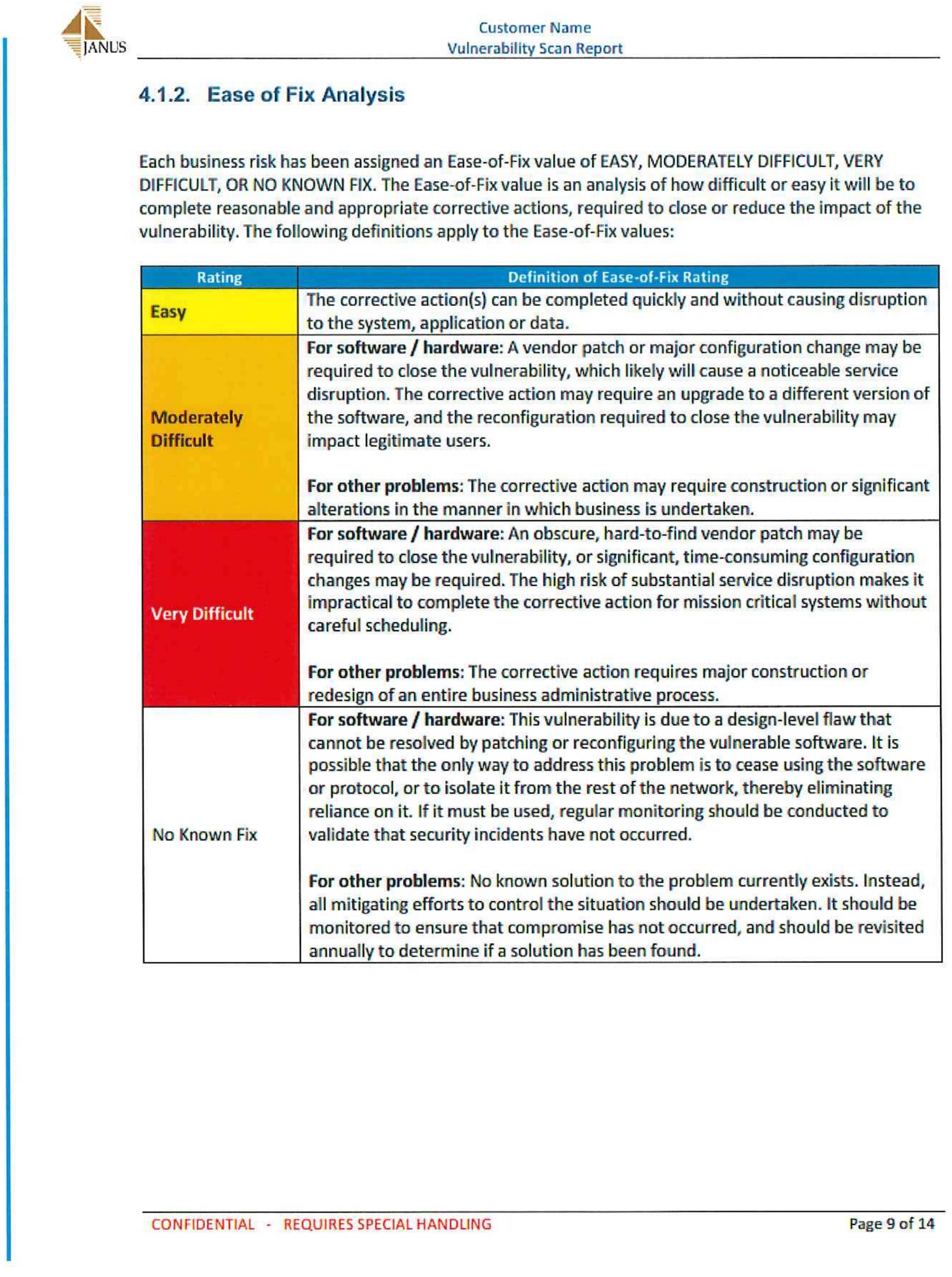
JANUS

Customer Name
Vulnerability Scan Report

HIGH Risk	Exploitation of the technical or procedural vulnerability will cause substantial harm. Significant political, financial and/or legal damage is likely to result. Security controls are not implemented effectively to reduce the severity of impact if the vulnerability were to be exploited. A technical vulnerability is a high risk when it is known to be exploitable and discoverable with well-known methods and the tools to do so are free and easy to obtain. A procedural vulnerability is a high risk when it is easily observed from outside the organization and employees are not trained to respond appropriately.
MEDIUM Risk	Exploitation of the technical or procedural vulnerability will cause noticeable harm. Exploitation of the vulnerability may cause moderate financial loss or public embarrassment. Security controls are in place to contain the severity of impact if the vulnerability were to be exploited, such that further political, financial or legal damage will not occur. The threat exposure is moderate-to-high. A technical vulnerability is moderate when it is known to be exploitable but the tools to discover or execute the vulnerability are not freely available or require expert technical skills to deploy. A procedural vulnerability is moderate when it can only be observed and executed from inside the organization and employees have some training to respond appropriately. Risks that would otherwise have a HIGH impact but have a limited threat exposure are also considered medium risks.
LOW Risk	Exploitation of the technical or procedural vulnerability will cause minimal impact to operations. Exploitation of the vulnerability may cause slight financial loss or service disruption. Security controls are in place to limit exploitation of the vulnerability. The threat exposure is moderate-to-low. A technical vulnerability is low when it is not widely known to be exploitable and there are no automated tools to discover or execute the vulnerability. Therefore, execution of the vulnerability would require expert technical skills. A procedural vulnerability is low when it can only be observed and executed on-site and employees have been trained to respond appropriately. Risks that would otherwise have a medium impact but have a limited threat exposure are also considered low risks.

CONFIDENTIAL - REQUIRES SPECIAL HANDLING

Page 8 of 14



Customer Name
Vulnerability Scan Report

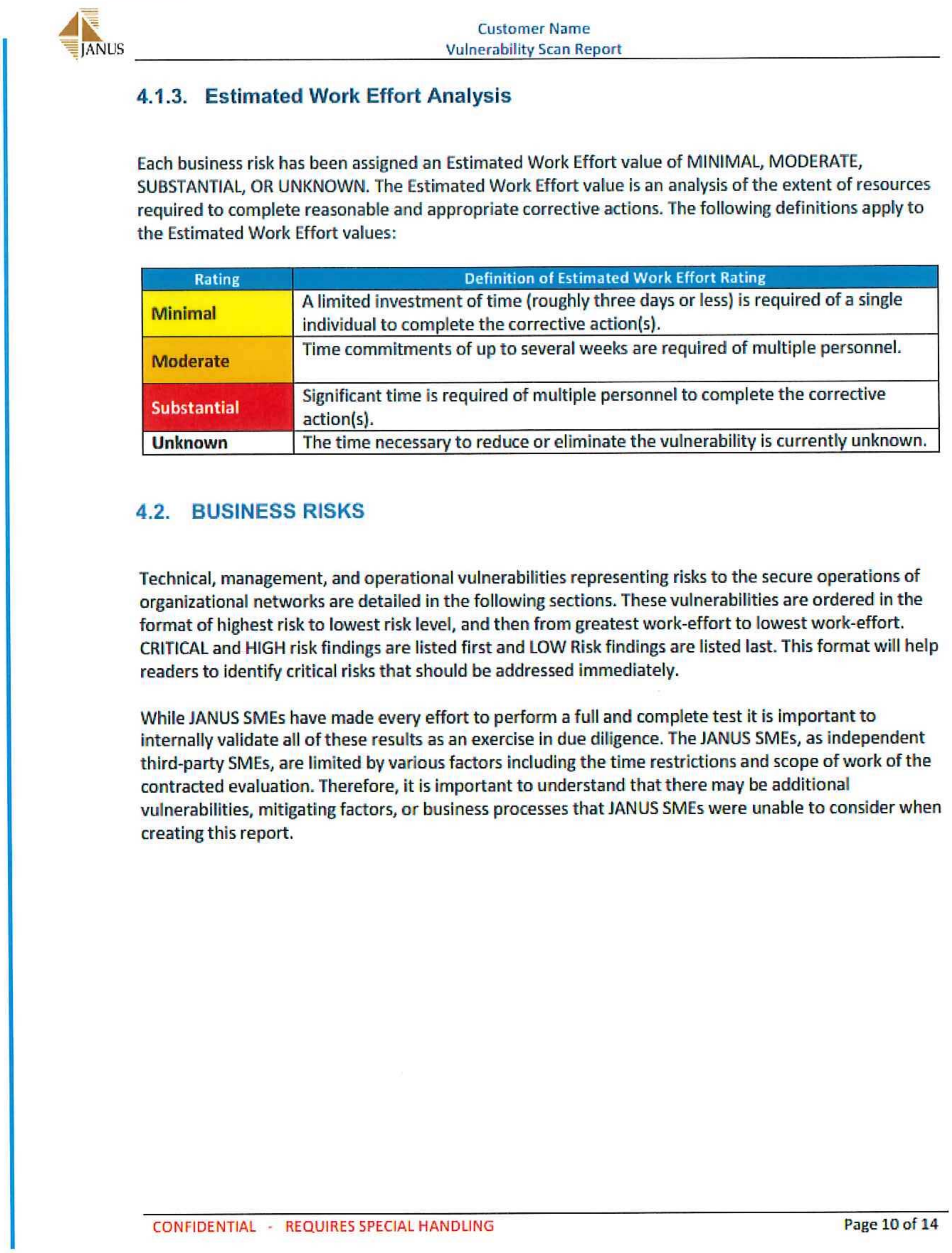
4.1.2. Ease of Fix Analysis

Each business risk has been assigned an Ease-of-Fix value of EASY, MODERATELY DIFFICULT, VERY DIFFICULT, OR NO KNOWN FIX. The Ease-of-Fix value is an analysis of how difficult or easy it will be to complete reasonable and appropriate corrective actions, required to close or reduce the impact of the vulnerability. The following definitions apply to the Ease-of-Fix values:

Rating	Definition of Ease-of-Fix Rating
Easy	The corrective action(s) can be completed quickly and without causing disruption to the system, application or data.
Moderately Difficult	**For software / hardware:** A vendor patch or major configuration change may be required to close the vulnerability, which likely will cause a noticeable service disruption. The corrective action may require an upgrade to a different version of the software, and the reconfiguration required to close the vulnerability may impact legitimate users. **For other problems:** The corrective action may require construction or significant alterations in the manner in which business is undertaken.
Very Difficult	**For software / hardware:** An obscure, hard-to-find vendor patch may be required to close the vulnerability, or significant, time-consuming configuration changes may be required. The high risk of substantial service disruption makes it impractical to complete the corrective action for mission critical systems without careful scheduling. **For other problems:** The corrective action requires major construction or redesign of an entire business administrative process.
No Known Fix	**For software / hardware:** This vulnerability is due to a design-level flaw that cannot be resolved by patching or reconfiguring the vulnerable software. It is possible that the only way to address this problem is to cease using the software or protocol, or to isolate it from the rest of the network, thereby eliminating reliance on it. If it must be used, regular monitoring should be conducted to validate that security incidents have not occurred. **For other problems:** No known solution to the problem currently exists. Instead, all mitigating efforts to control the situation should be undertaken. It should be monitored to ensure that compromise has not occurred, and should be revisited annually to determine if a solution has been found.

CONFIDENTIAL - REQUIRES SPECIAL HANDLING

Page 9 of 14



4.1.3. Estimated Work Effort Analysis

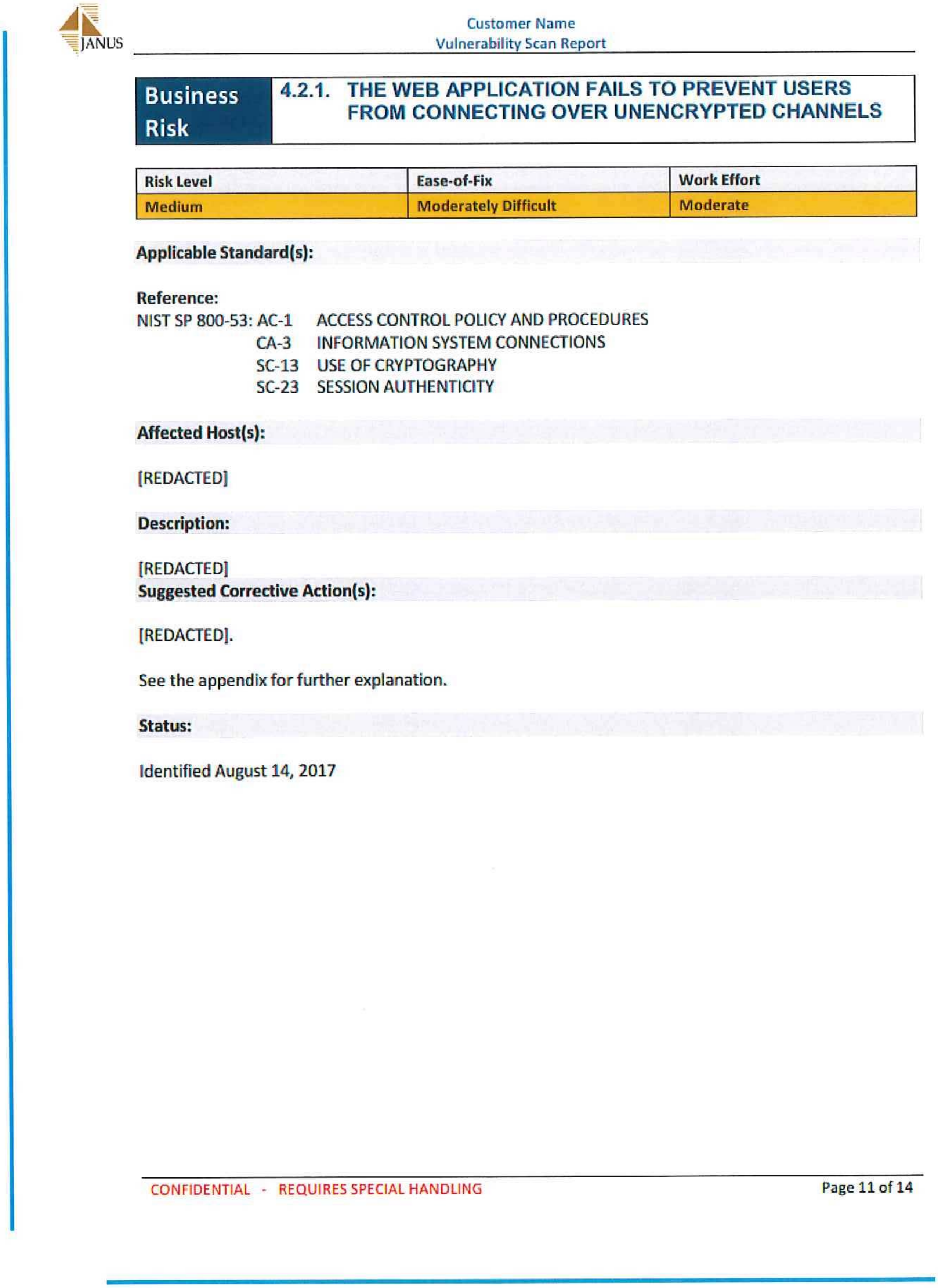
Each business risk has been assigned an Estimated Work Effort value of MINIMAL, MODERATE, SUBSTANTIAL, OR UNKNOWN. The Estimated Work Effort value is an analysis of the extent of resources required to complete reasonable and appropriate corrective actions. The following definitions apply to the Estimated Work Effort values:

Rating	Definition of Estimated Work Effort Rating
Minimal	A limited investment of time (roughly three days or less) is required of a single individual to complete the corrective action(s).
Moderate	Time commitments of up to several weeks are required of multiple personnel.
Substantial	Significant time is required of multiple personnel to complete the corrective action(s).
Unknown	The time necessary to reduce or eliminate the vulnerability is currently unknown.

4.2. BUSINESS RISKS

Technical, management, and operational vulnerabilities representing risks to the secure operations of organizational networks are detailed in the following sections. These vulnerabilities are ordered in the format of highest risk to lowest risk level, and then from greatest work-effort to lowest work-effort. CRITICAL and HIGH risk findings are listed first and LOW Risk findings are listed last. This format will help readers to identify critical risks that should be addressed immediately.

While JANUS SMEs have made every effort to perform a full and complete test it is important to internally validate all of these results as an exercise in due diligence. The JANUS SMEs, as independent third-party SMEs, are limited by various factors including the time restrictions and scope of work of the contracted evaluation. Therefore, it is important to understand that there may be additional vulnerabilities, mitigating factors, or business processes that JANUS SMEs were unable to consider when creating this report.



Customer Name
Vulnerability Scan Report

Business Risk — 4.2.1. THE WEB APPLICATION FAILS TO PREVENT USERS FROM CONNECTING OVER UNENCRYPTED CHANNELS

Risk Level	Ease-of-Fix	Work Effort
Medium	Moderately Difficult	Moderate

Applicable Standard(s):

Reference:

NIST SP 800-53:	AC-1	ACCESS CONTROL POLICY AND PROCEDURES
	CA-3	INFORMATION SYSTEM CONNECTIONS
	SC-13	USE OF CRYPTOGRAPHY
	SC-23	SESSION AUTHENTICITY

Affected Host(s):

[REDACTED]

Description:

[REDACTED]

Suggested Corrective Action(s):

[REDACTED].

See the appendix for further explanation.

Status:

Identified August 14, 2017

CONFIDENTIAL - REQUIRES SPECIAL HANDLING

Page 11 of 14

Business Risk — 4.2.2. WEB APPLICATIONS ALLOW SENSITIVE INFORMATION TO BE INTERCEPTED

Risk Level	Ease-of-Fix	Work Effort
High	Moderately Difficult	Moderate

Applicable Standard(s):

Reference:
NIST SP 800-53: MP-4 MEDIA STORAGE
MP-5 MEDIA TRANSPORT
SC-8 TRANSMISSION INTEGRITY

Affected Host(s):

[REDACTED]
Description:

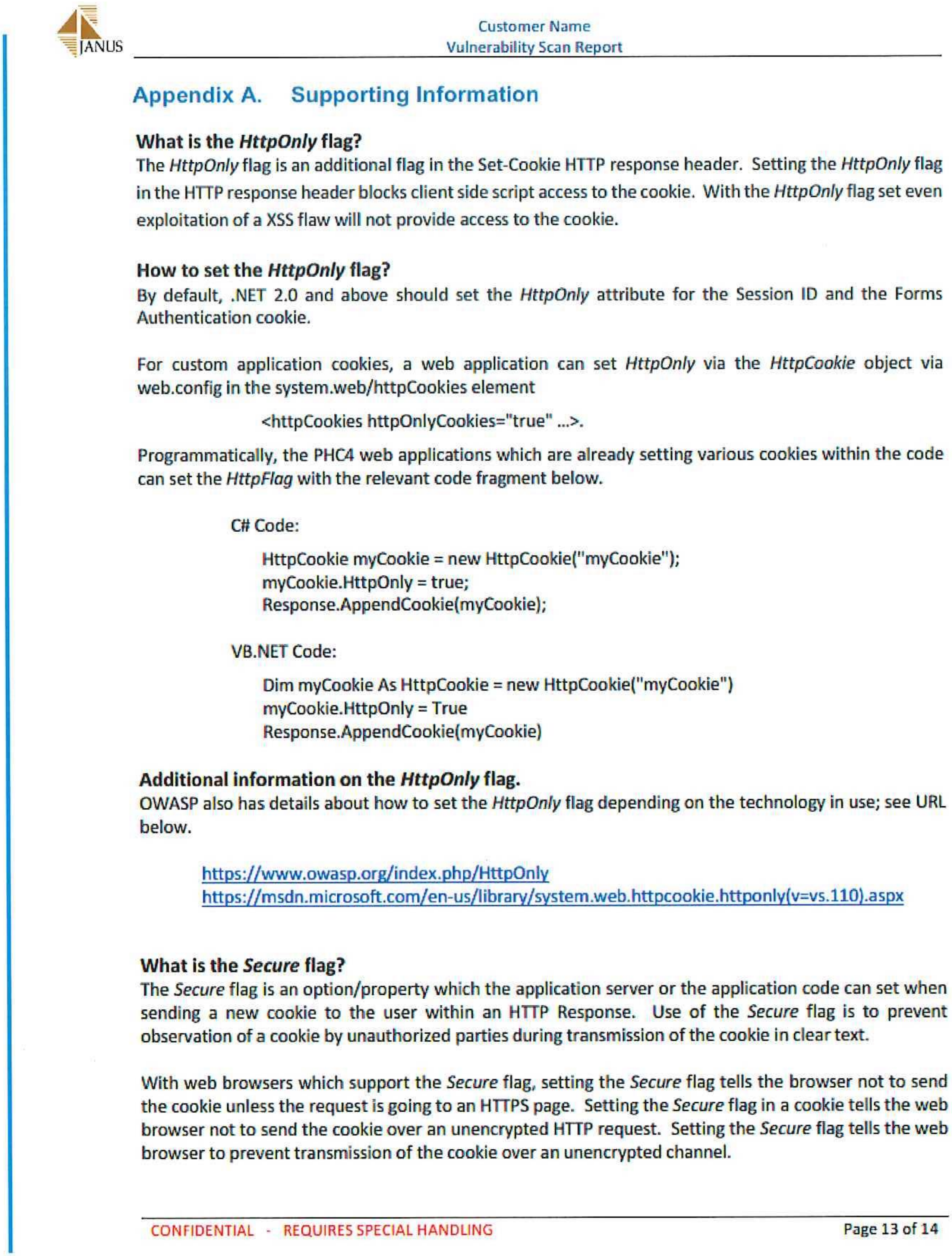
[REDACTED]
Suggested Corrective Action(s):

[REDACTED]other serious attacks can be delivered by client-side script injection, aside from simple cookie stealing.

See the appendix for further explanation.

Status:

Identified August 14, 2017



Appendix A. Supporting Information

What is the *HttpOnly* flag?

The *HttpOnly* flag is an additional flag in the Set-Cookie HTTP response header. Setting the *HttpOnly* flag in the HTTP response header blocks client side script access to the cookie. With the *HttpOnly* flag set even exploitation of a XSS flaw will not provide access to the cookie.

How to set the *HttpOnly* flag?

By default, .NET 2.0 and above should set the *HttpOnly* attribute for the Session ID and the Forms Authentication cookie.

For custom application cookies, a web application can set *HttpOnly* via the *HttpCookie* object via web.config in the system.web/httpCookies element

```
<httpCookies httpOnlyCookies="true" ...>.
```

Programmatically, the PHC4 web applications which are already setting various cookies within the code can set the *HttpFlag* with the relevant code fragment below.

C# Code:

```
HttpCookie myCookie = new HttpCookie("myCookie");
myCookie.HttpOnly = true;
Response.AppendCookie(myCookie);
```

VB.NET Code:

```
Dim myCookie As HttpCookie = new HttpCookie("myCookie")
myCookie.HttpOnly = True
Response.AppendCookie(myCookie)
```

Additional information on the *HttpOnly* flag.

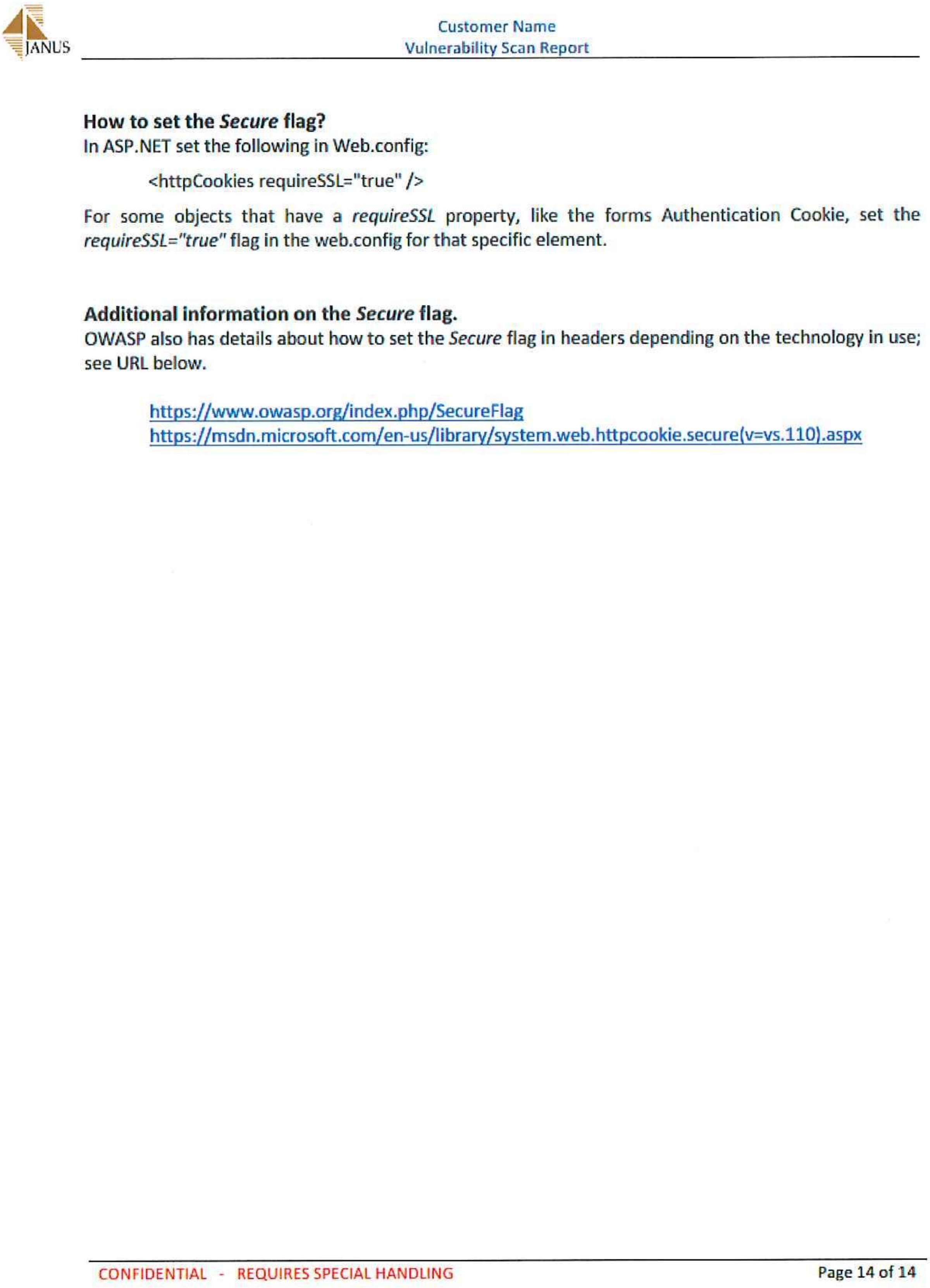
OWASP also has details about how to set the *HttpOnly* flag depending on the technology in use; see URL below.

https://www.owasp.org/index.php/HttpOnly
https://msdn.microsoft.com/en-us/library/system.web.httpcookie.httponly(v=vs.110).aspx

What is the *Secure* flag?

The *Secure* flag is an option/property which the application server or the application code can set when sending a new cookie to the user within an HTTP Response. Use of the *Secure* flag is to prevent observation of a cookie by unauthorized parties during transmission of the cookie in clear text.

With web browsers which support the *Secure* flag, setting the *Secure* flag tells the browser not to send the cookie unless the request is going to an HTTPS page. Setting the *Secure* flag in a cookie tells the web browser not to send the cookie over an unencrypted HTTP request. Setting the *Secure* flag tells the web browser to prevent transmission of the cookie over an unencrypted channel.



How to set the *Secure* flag?

In ASP.NET set the following in Web.config:

```
<httpCookies requireSSL="true" />
```

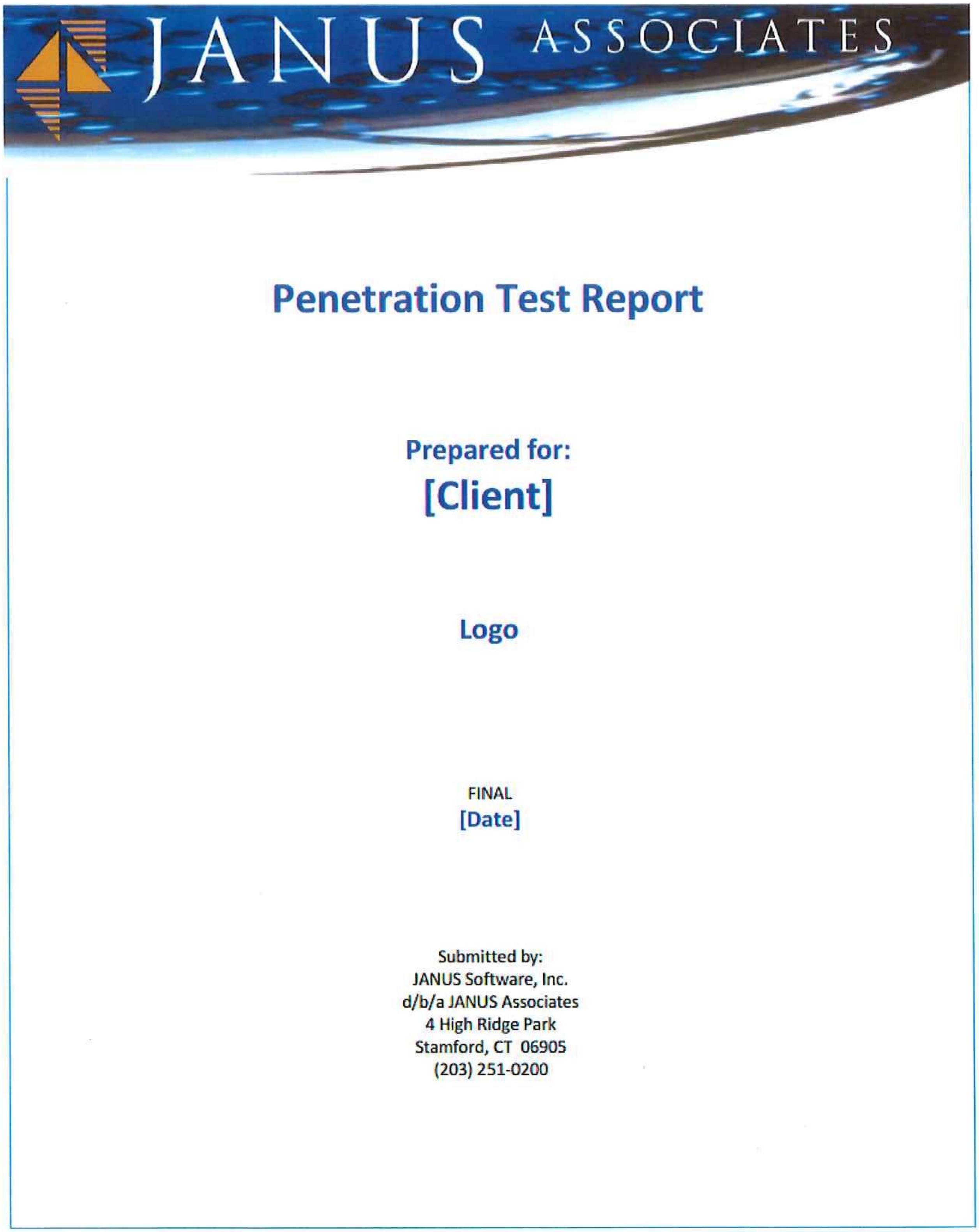
For some objects that have a *requireSSL* property, like the forms Authentication Cookie, set the *requireSSL="true"* flag in the web.config for that specific element.

Additional information on the *Secure* flag.

OWASP also has details about how to set the *Secure* flag in headers depending on the technology in use; see URL below.

https://www.owasp.org/index.php/SecureFlag
https://msdn.microsoft.com/en-us/library/system.web.httpcookie.secure(v=vs.110).aspx

Penetration Testing



Penetration Test Report

Prepared for:
[Client]

Logo

FINAL
[Date]

Submitted by:
JANUS Software, Inc.
d/b/a JANUS Associates
4 High Ridge Park
Stamford, CT 06905
(203) 251-0200

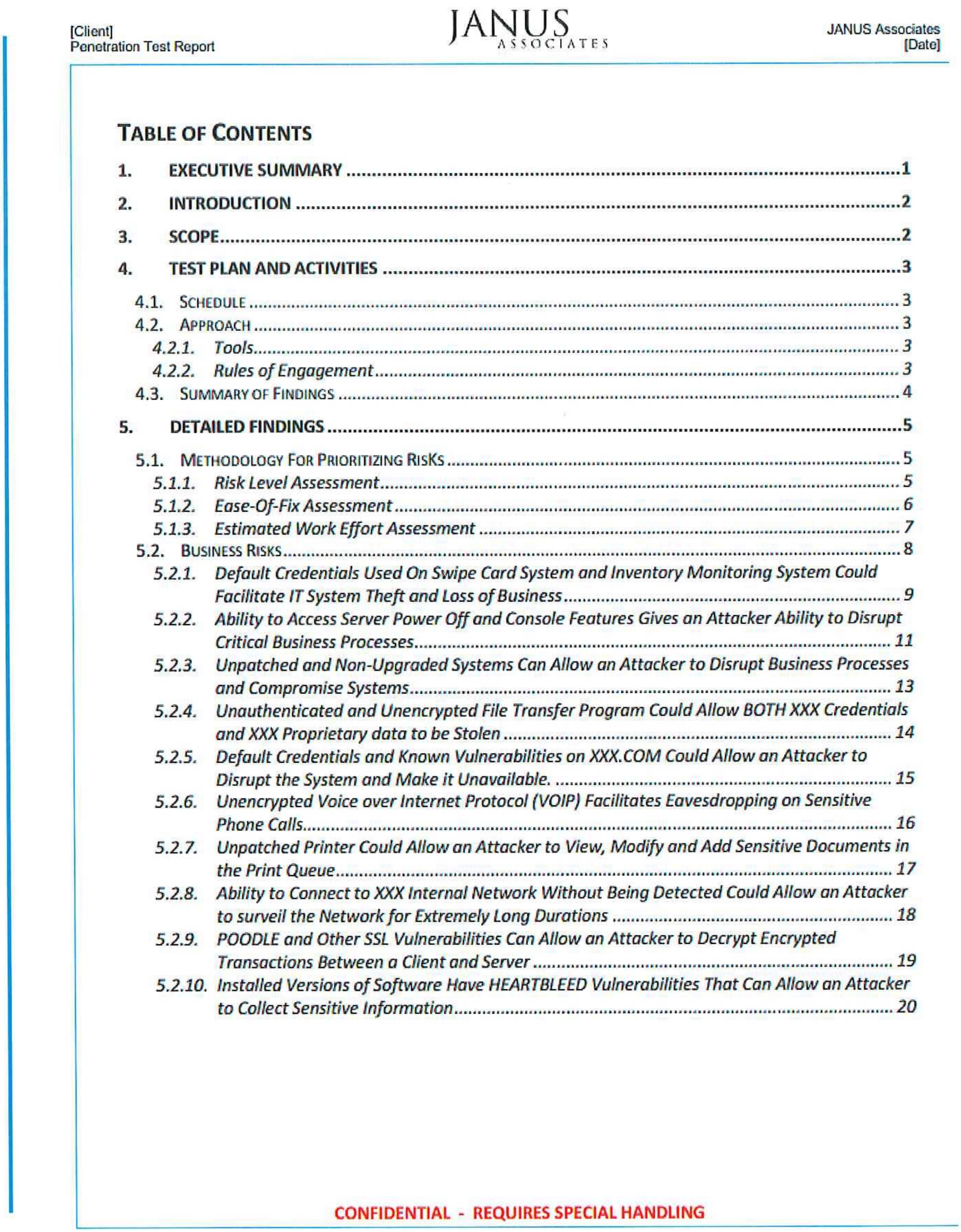
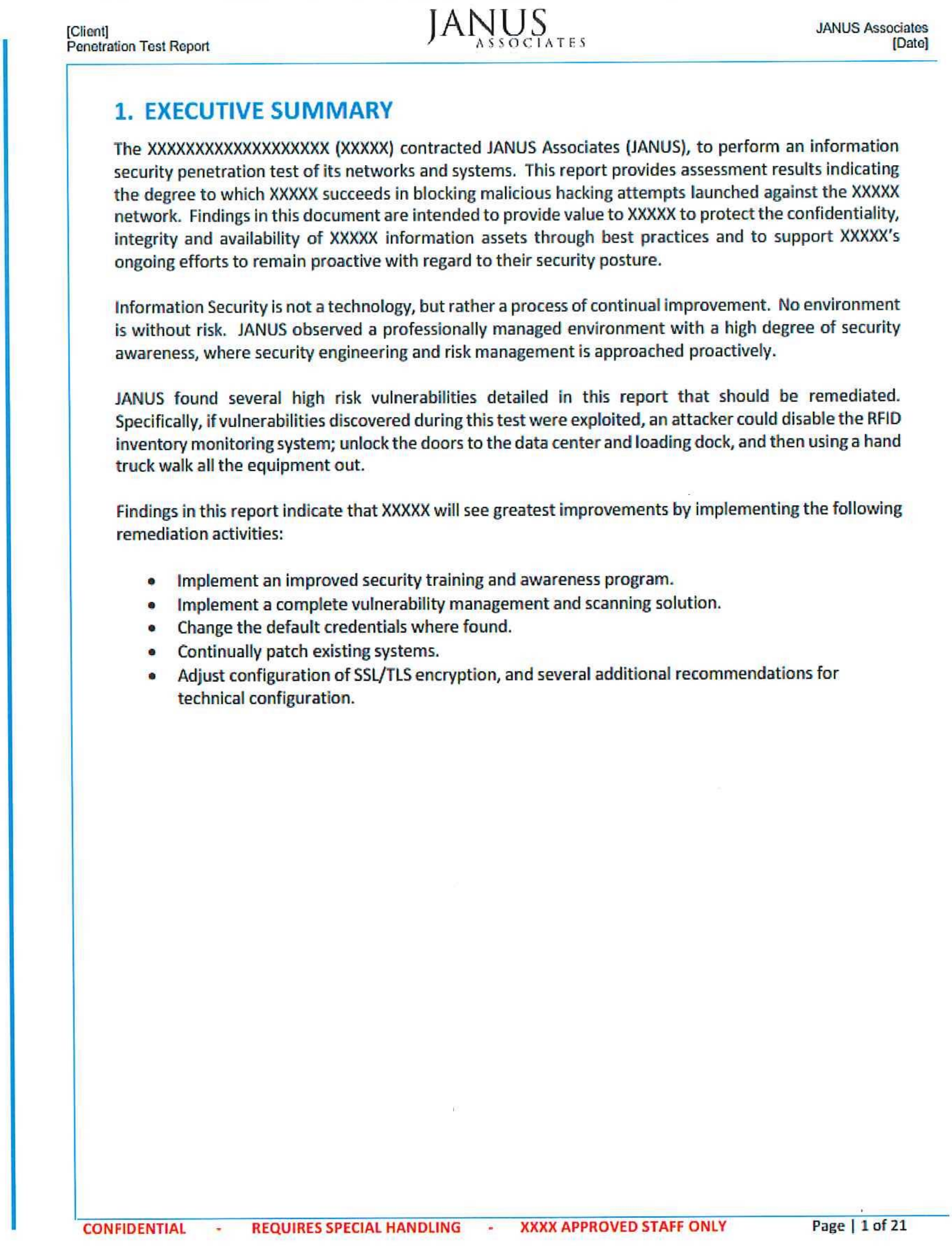


TABLE OF CONTENTS

CONFIDENTIAL - REQUIRES SPECIAL HANDLING



[Client]
Penetration Test Report

JANUS ASSOCIATES

JANUS Associates
[Date]

1. EXECUTIVE SUMMARY

The XXXXXXXXXXXXXXXXXXX (XXXXX) contracted JANUS Associates (JANUS), to perform an information security penetration test of its networks and systems. This report provides assessment results indicating the degree to which XXXXX succeeds in blocking malicious hacking attempts launched against the XXXXX network. Findings in this document are intended to provide value to XXXXX to protect the confidentiality, integrity and availability of XXXXX information assets through best practices and to support XXXXX's ongoing efforts to remain proactive with regard to their security posture.

Information Security is not a technology, but rather a process of continual improvement. No environment is without risk. JANUS observed a professionally managed environment with a high degree of security awareness, where security engineering and risk management is approached proactively.

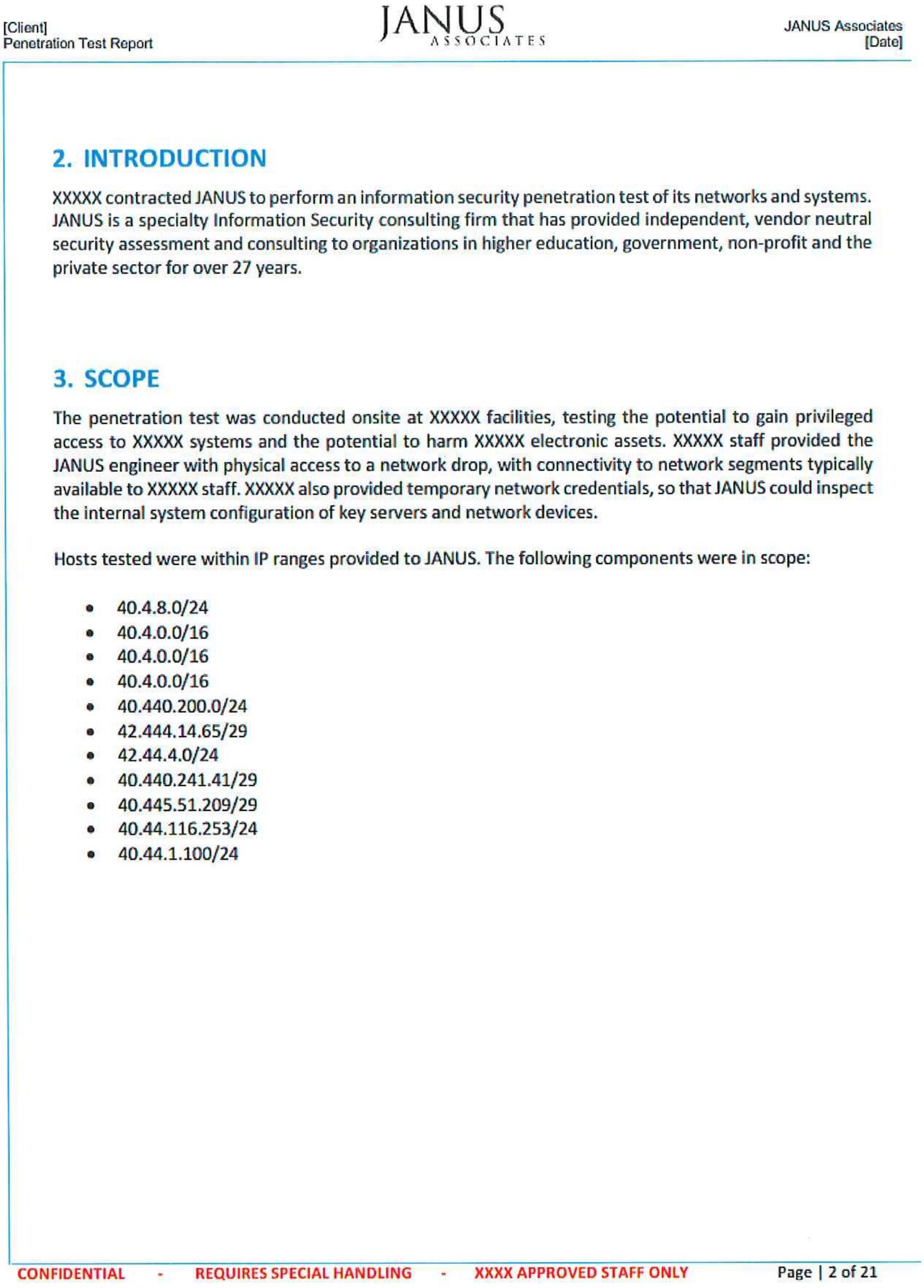
JANUS found several high risk vulnerabilities detailed in this report that should be remediated. Specifically, if vulnerabilities discovered during this test were exploited, an attacker could disable the RFID inventory monitoring system; unlock the doors to the data center and loading dock, and then using a hand truck walk all the equipment out.

Findings in this report indicate that XXXXX will see greatest improvements by implementing the following remediation activities:

- Implement an improved security training and awareness program.
- Implement a complete vulnerability management and scanning solution.
- Change the default credentials where found.
- Continually patch existing systems.
- Adjust configuration of SSL/TLS encryption, and several additional recommendations for technical configuration.

CONFIDENTIAL - REQUIRES SPECIAL HANDLING - XXXX APPROVED STAFF ONLY

Page | 1 of 21



2. INTRODUCTION

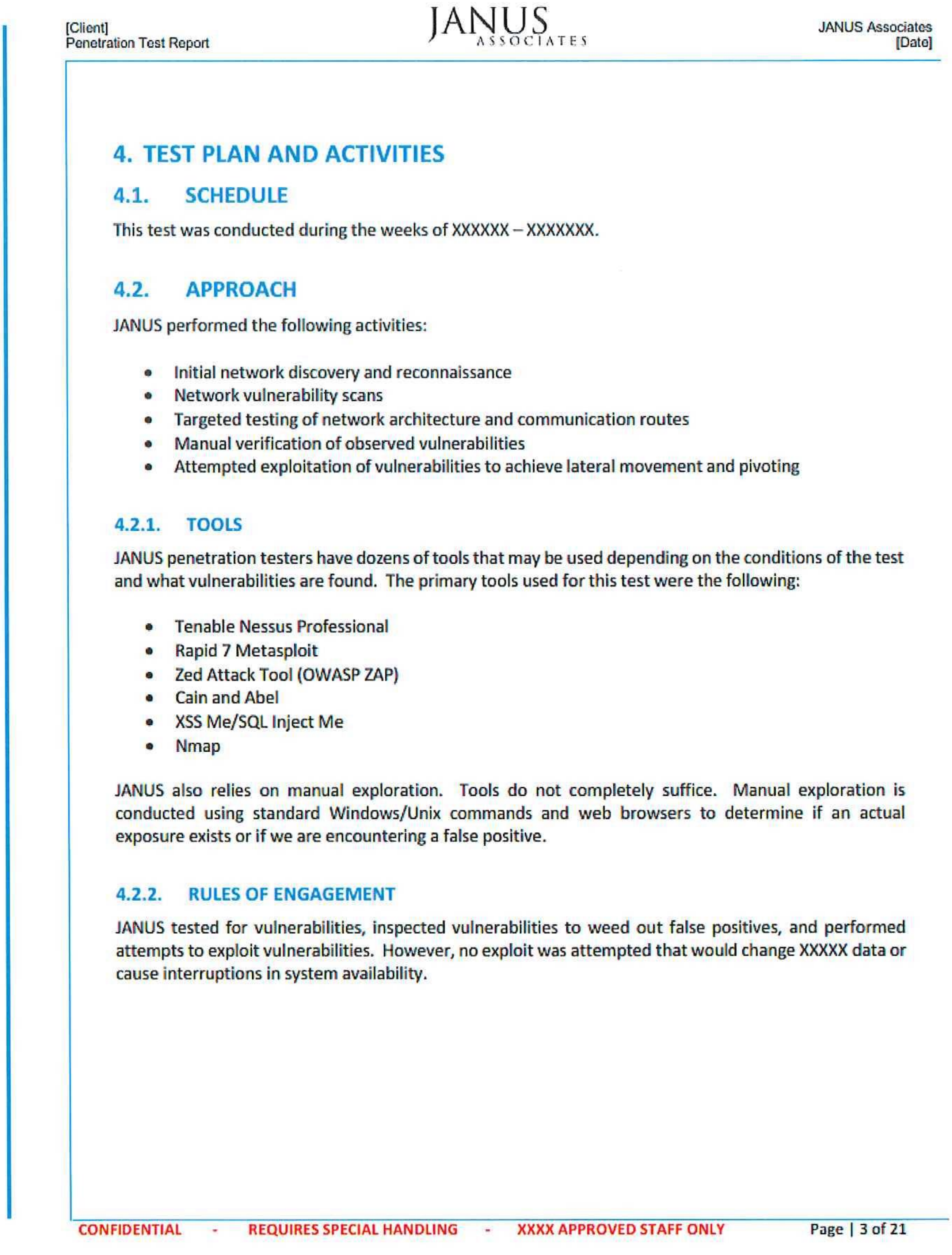
XXXXX contracted JANUS to perform an information security penetration test of its networks and systems. JANUS is a specialty Information Security consulting firm that has provided independent, vendor neutral security assessment and consulting to organizations in higher education, government, non-profit and the private sector for over 27 years.

3. SCOPE

The penetration test was conducted onsite at XXXXX facilities, testing the potential to gain privileged access to XXXXX systems and the potential to harm XXXXX electronic assets. XXXXX staff provided the JANUS engineer with physical access to a network drop, with connectivity to network segments typically available to XXXXX staff. XXXXX also provided temporary network credentials, so that JANUS could inspect the internal system configuration of key servers and network devices.

Hosts tested were within IP ranges provided to JANUS. The following components were in scope:

- 40.4.8.0/24
- 40.4.0.0/16
- 40.4.0.0/16
- 40.4.0.0/16
- 40.440.200.0/24
- 42.444.14.65/29
- 42.44.4.0/24
- 40.440.241.41/29
- 40.445.51.209/29
- 40.44.116.253/24
- 40.44.1.100/24



4. TEST PLAN AND ACTIVITIES

4.1. SCHEDULE

This test was conducted during the weeks of XXXXXX – XXXXXXX.

4.2. APPROACH

JANUS performed the following activities:

- Initial network discovery and reconnaissance
- Network vulnerability scans
- Targeted testing of network architecture and communication routes
- Manual verification of observed vulnerabilities
- Attempted exploitation of vulnerabilities to achieve lateral movement and pivoting

4.2.1. TOOLS

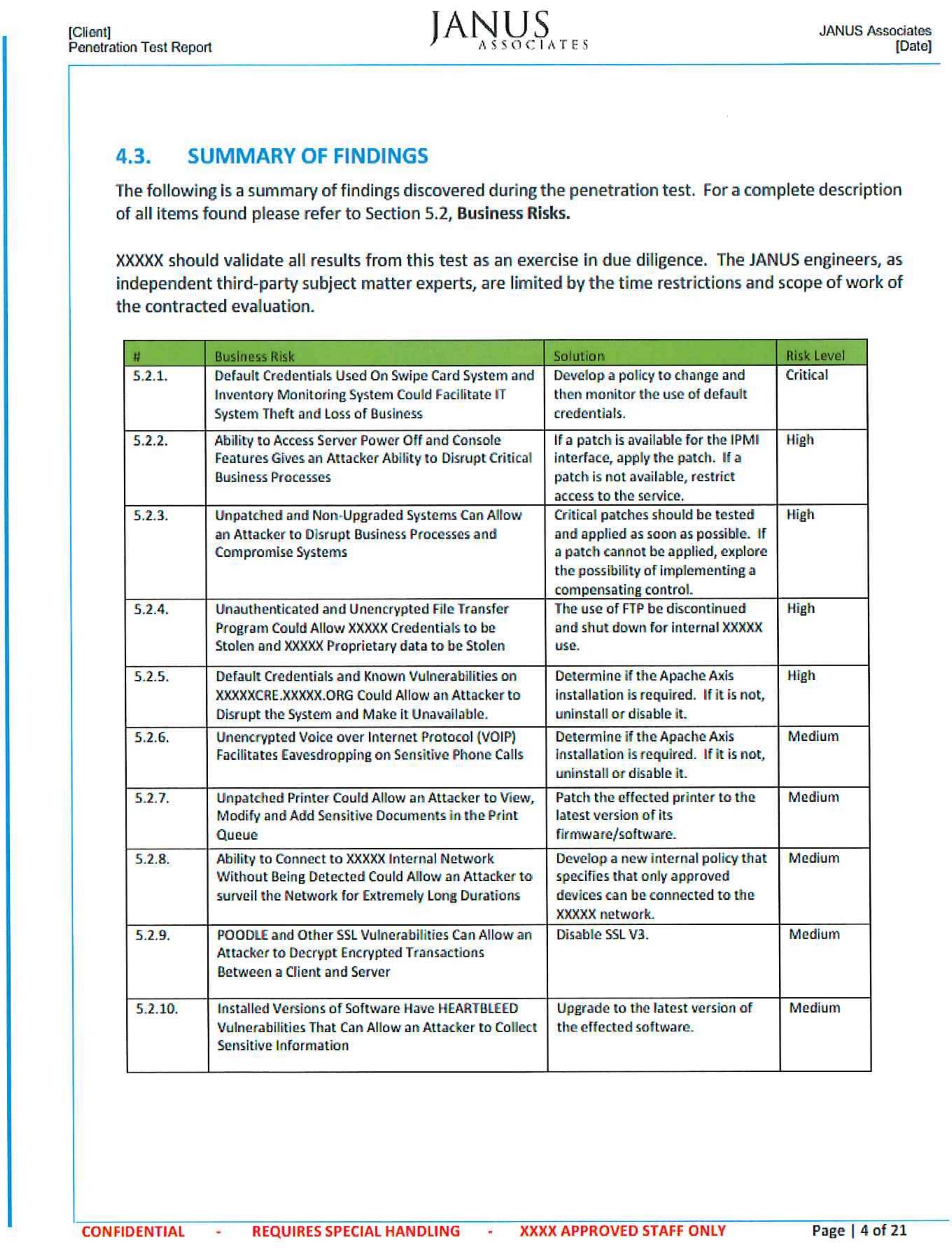
JANUS penetration testers have dozens of tools that may be used depending on the conditions of the test and what vulnerabilities are found. The primary tools used for this test were the following:

- Tenable Nessus Professional
- Rapid 7 Metasploit
- Zed Attack Tool (OWASP ZAP)
- Cain and Abel
- XSS Me/SQL Inject Me
- Nmap

JANUS also relies on manual exploration. Tools do not completely suffice. Manual exploration is conducted using standard Windows/Unix commands and web browsers to determine if an actual exposure exists or if we are encountering a false positive.

4.2.2. RULES OF ENGAGEMENT

JANUS tested for vulnerabilities, inspected vulnerabilities to weed out false positives, and performed attempts to exploit vulnerabilities. However, no exploit was attempted that would change XXXXX data or cause interruptions in system availability.

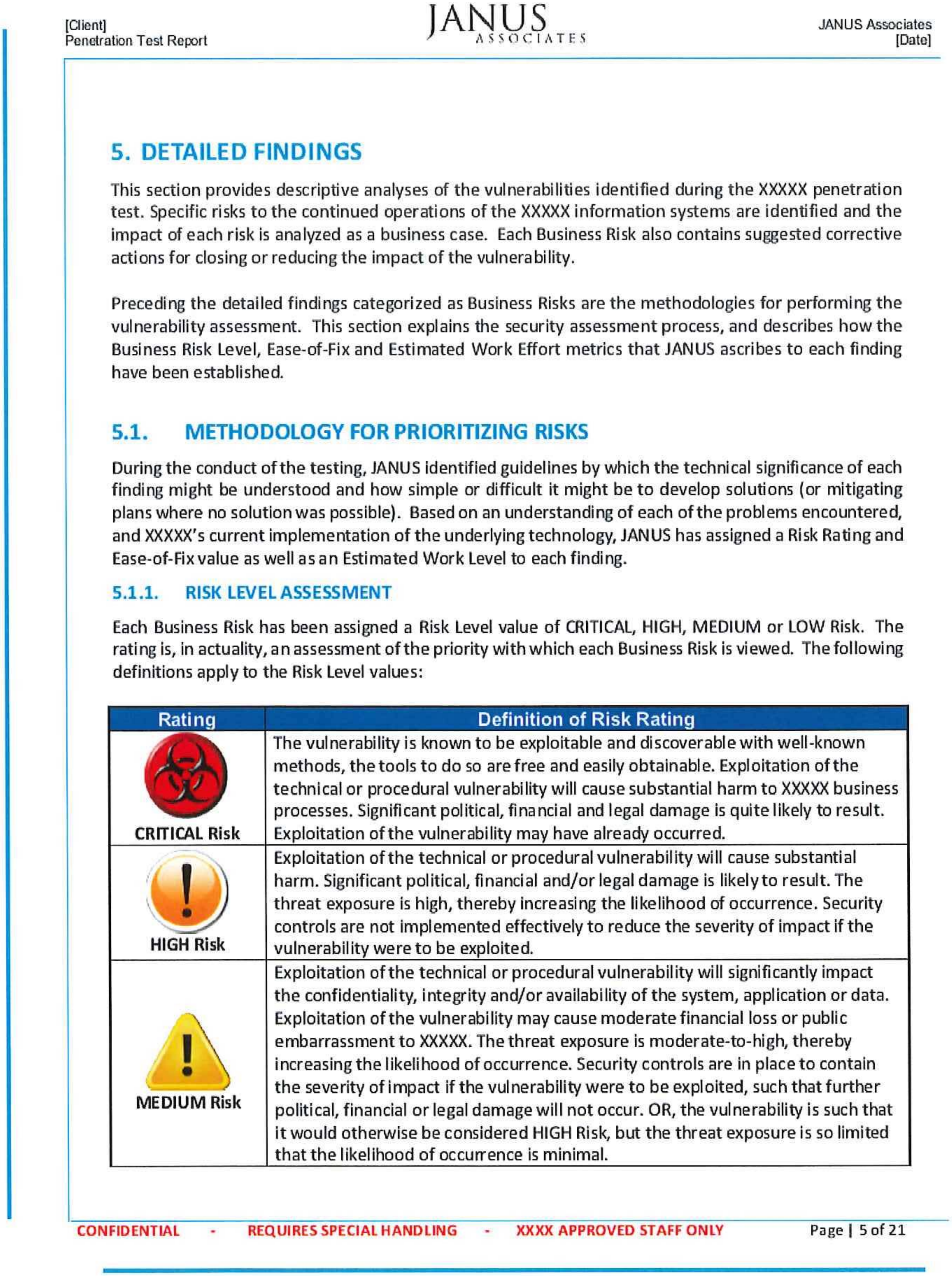


4.3. SUMMARY OF FINDINGS

The following is a summary of findings discovered during the penetration test. For a complete description of all items found please refer to Section 5.2, **Business Risks.**

XXXXX should validate all results from this test as an exercise in due diligence. The JANUS engineers, as independent third-party subject matter experts, are limited by the time restrictions and scope of work of the contracted evaluation.

#	Business Risk	Solution	Risk Level
5.2.1.	Default Credentials Used On Swipe Card System and Inventory Monitoring System Could Facilitate IT System Theft and Loss of Business	Develop a policy to change and then monitor the use of default credentials.	Critical
5.2.2.	Ability to Access Server Power Off and Console Features Gives an Attacker Ability to Disrupt Critical Business Processes	If a patch is available for the IPMI interface, apply the patch. If a patch is not available, restrict access to the service.	High
5.2.3.	Unpatched and Non-Upgraded Systems Can Allow an Attacker to Disrupt Business Processes and Compromise Systems	Critical patches should be tested and applied as soon as possible. If a patch cannot be applied, explore the possibility of implementing a compensating control.	High
5.2.4.	Unauthenticated and Unencrypted File Transfer Program Could Allow XXXXX Credentials to be Stolen and XXXXX Proprietary data to be Stolen	The use of FTP be discontinued and shut down for internal XXXXX use.	High
5.2.5.	Default Credentials and Known Vulnerabilities on XXXXXCRE.XXXXX.ORG Could Allow an Attacker to Disrupt the System and Make it Unavailable.	Determine if the Apache Axis installation is required. If it is not, uninstall or disable it.	High
5.2.6.	Unencrypted Voice over Internet Protocol (VOIP) Facilitates Eavesdropping on Sensitive Phone Calls	Determine if the Apache Axis installation is required. If it is not, uninstall or disable it.	Medium
5.2.7.	Unpatched Printer Could Allow an Attacker to View, Modify and Add Sensitive Documents in the Print Queue	Patch the effected printer to the latest version of its firmware/software.	Medium
5.2.8.	Ability to Connect to XXXXX Internal Network Without Being Detected Could Allow an Attacker to surveil the Network for Extremely Long Durations	Develop a new internal policy that specifies that only approved devices can be connected to the XXXXX network.	Medium
5.2.9.	POODLE and Other SSL Vulnerabilities Can Allow an Attacker to Decrypt Encrypted Transactions Between a Client and Server	Disable SSL V3.	Medium
5.2.10.	Installed Versions of Software Have HEARTBLEED Vulnerabilities That Can Allow an Attacker to Collect Sensitive Information	Upgrade to the latest version of the effected software.	Medium



5. DETAILED FINDINGS

This section provides descriptive analyses of the vulnerabilities identified during the XXXXX penetration test. Specific risks to the continued operations of the XXXXX information systems are identified and the impact of each risk is analyzed as a business case. Each Business Risk also contains suggested corrective actions for closing or reducing the impact of the vulnerability.

Preceding the detailed findings categorized as Business Risks are the methodologies for performing the vulnerability assessment. This section explains the security assessment process, and describes how the Business Risk Level, Ease-of-Fix and Estimated Work Effort metrics that JANUS ascribes to each finding have been established.

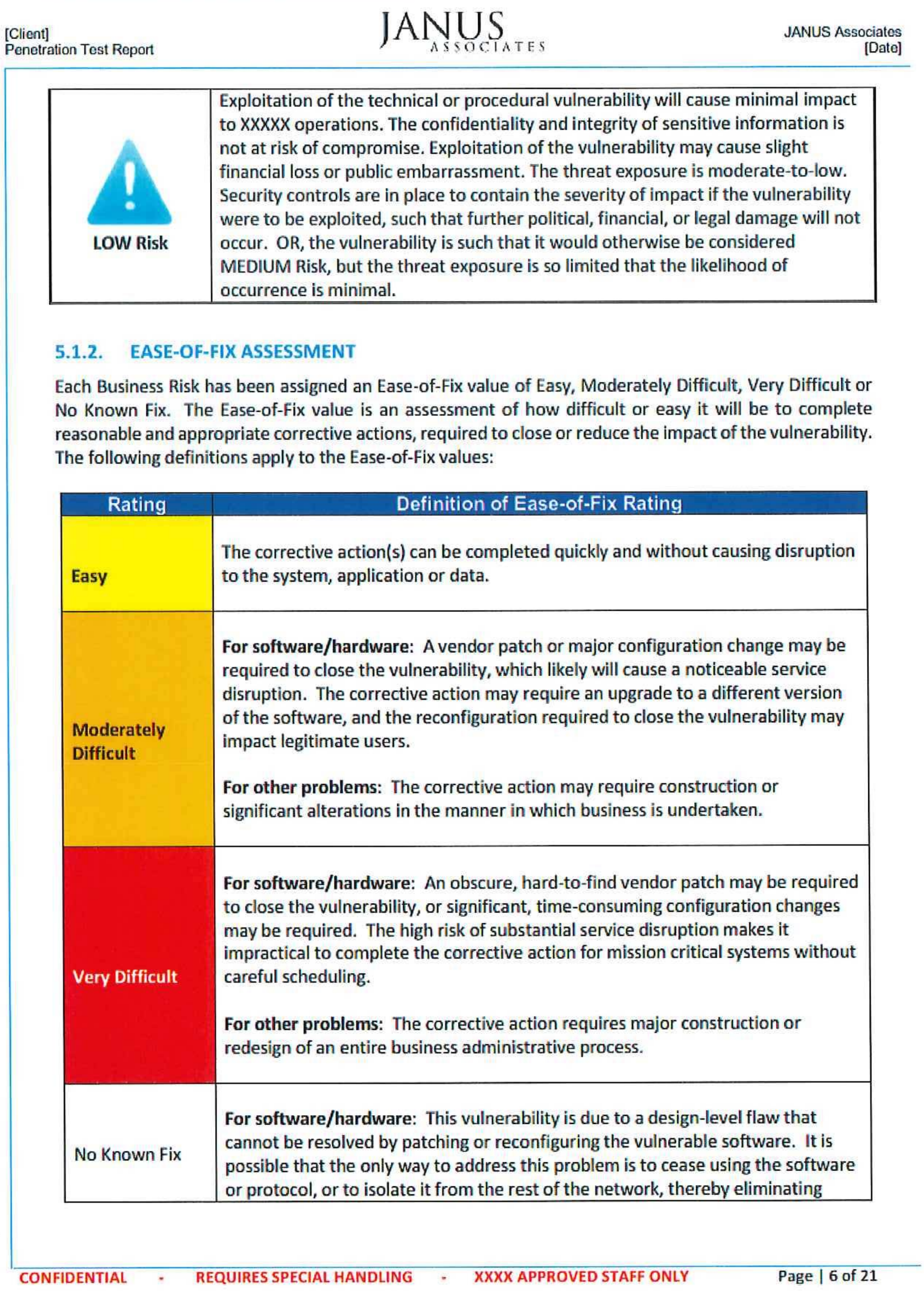
5.1. METHODOLOGY FOR PRIORITIZING RISKS

During the conduct of the testing, JANUS identified guidelines by which the technical significance of each finding might be understood and how simple or difficult it might be to develop solutions (or mitigating plans where no solution was possible). Based on an understanding of each of the problems encountered, and XXXXX's current implementation of the underlying technology, JANUS has assigned a Risk Rating and Ease-of-Fix value as well as an Estimated Work Level to each finding.

5.1.1. RISK LEVEL ASSESSMENT

Each Business Risk has been assigned a Risk Level value of CRITICAL, HIGH, MEDIUM or LOW Risk. The rating is, in actuality, an assessment of the priority with which each Business Risk is viewed. The following definitions apply to the Risk Level values:

Rating	Definition of Risk Rating
☣ **CRITICAL Risk**	The vulnerability is known to be exploitable and discoverable with well-known methods, the tools to do so are free and easily obtainable. Exploitation of the technical or procedural vulnerability will cause substantial harm to XXXXX business processes. Significant political, financial and legal damage is quite likely to result. Exploitation of the vulnerability may have already occurred.
❗ **HIGH Risk**	Exploitation of the technical or procedural vulnerability will cause substantial harm. Significant political, financial and/or legal damage is likely to result. The threat exposure is high, thereby increasing the likelihood of occurrence. Security controls are not implemented effectively to reduce the severity of impact if the vulnerability were to be exploited.
⚠ **MEDIUM Risk**	Exploitation of the technical or procedural vulnerability will significantly impact the confidentiality, integrity and/or availability of the system, application or data. Exploitation of the vulnerability may cause moderate financial loss or public embarrassment to XXXXX. The threat exposure is moderate-to-high, thereby increasing the likelihood of occurrence. Security controls are in place to contain the severity of impact if the vulnerability were to be exploited, such that further political, financial or legal damage will not occur. OR, the vulnerability is such that it would otherwise be considered HIGH Risk, but the threat exposure is so limited that the likelihood of occurrence is minimal.

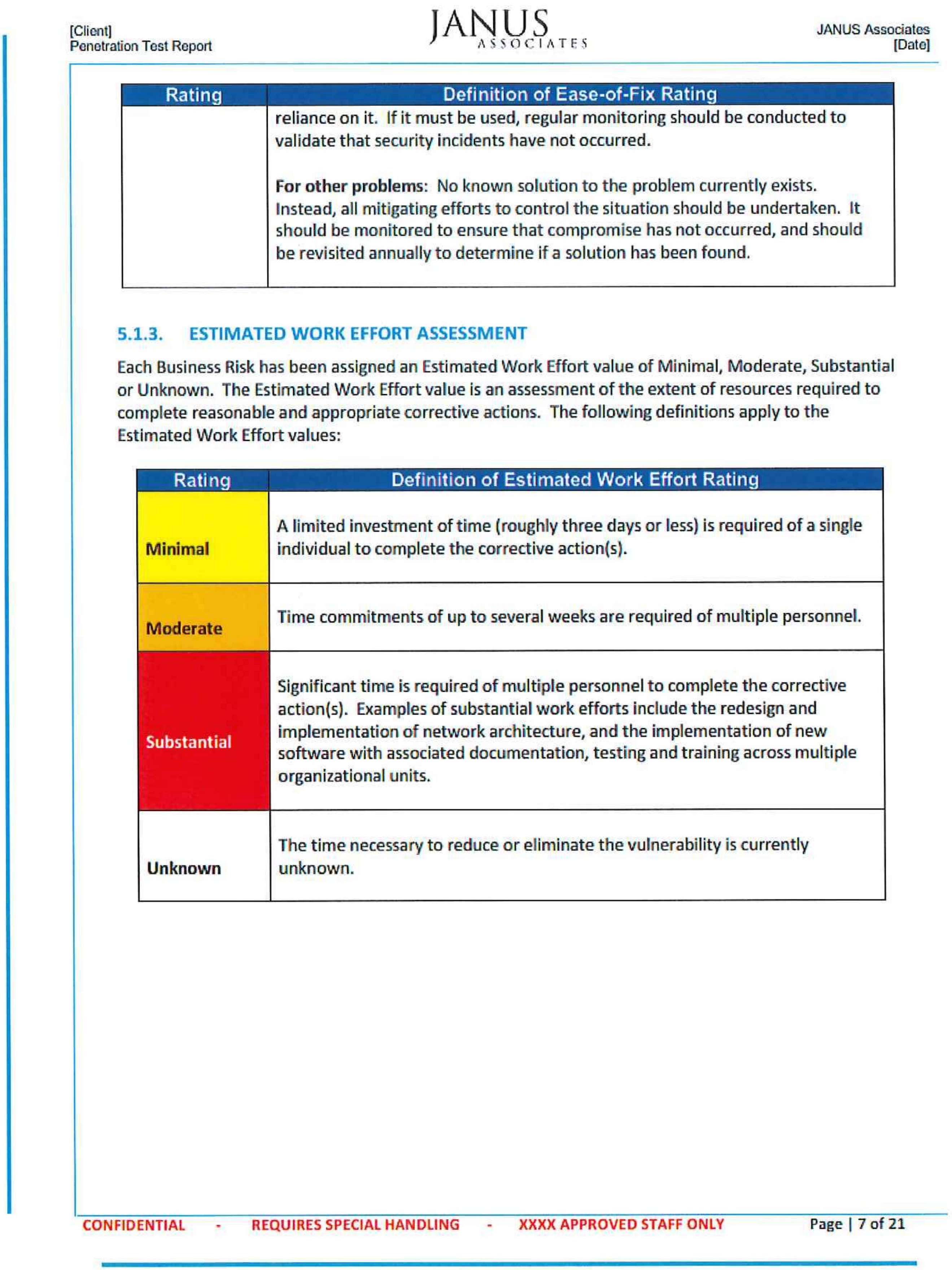


⚠ **LOW Risk**	Exploitation of the technical or procedural vulnerability will cause minimal impact to XXXXX operations. The confidentiality and integrity of sensitive information is not at risk of compromise. Exploitation of the vulnerability may cause slight financial loss or public embarrassment. The threat exposure is moderate-to-low. Security controls are in place to contain the severity of impact if the vulnerability were to be exploited, such that further political, financial, or legal damage will not occur. OR, the vulnerability is such that it would otherwise be considered MEDIUM Risk, but the threat exposure is so limited that the likelihood of occurrence is minimal.

5.1.2. EASE-OF-FIX ASSESSMENT

Each Business Risk has been assigned an Ease-of-Fix value of Easy, Moderately Difficult, Very Difficult or No Known Fix. The Ease-of-Fix value is an assessment of how difficult or easy it will be to complete reasonable and appropriate corrective actions, required to close or reduce the impact of the vulnerability. The following definitions apply to the Ease-of-Fix values:

Rating	Definition of Ease-of-Fix Rating
Easy	The corrective action(s) can be completed quickly and without causing disruption to the system, application or data.
Moderately Difficult	**For software/hardware:** A vendor patch or major configuration change may be required to close the vulnerability, which likely will cause a noticeable service disruption. The corrective action may require an upgrade to a different version of the software, and the reconfiguration required to close the vulnerability may impact legitimate users. **For other problems:** The corrective action may require construction or significant alterations in the manner in which business is undertaken.
Very Difficult	**For software/hardware:** An obscure, hard-to-find vendor patch may be required to close the vulnerability, or significant, time-consuming configuration changes may be required. The high risk of substantial service disruption makes it impractical to complete the corrective action for mission critical systems without careful scheduling. **For other problems:** The corrective action requires major construction or redesign of an entire business administrative process.
No Known Fix	**For software/hardware:** This vulnerability is due to a design-level flaw that cannot be resolved by patching or reconfiguring the vulnerable software. It is possible that the only way to address this problem is to cease using the software or protocol, or to isolate it from the rest of the network, thereby eliminating

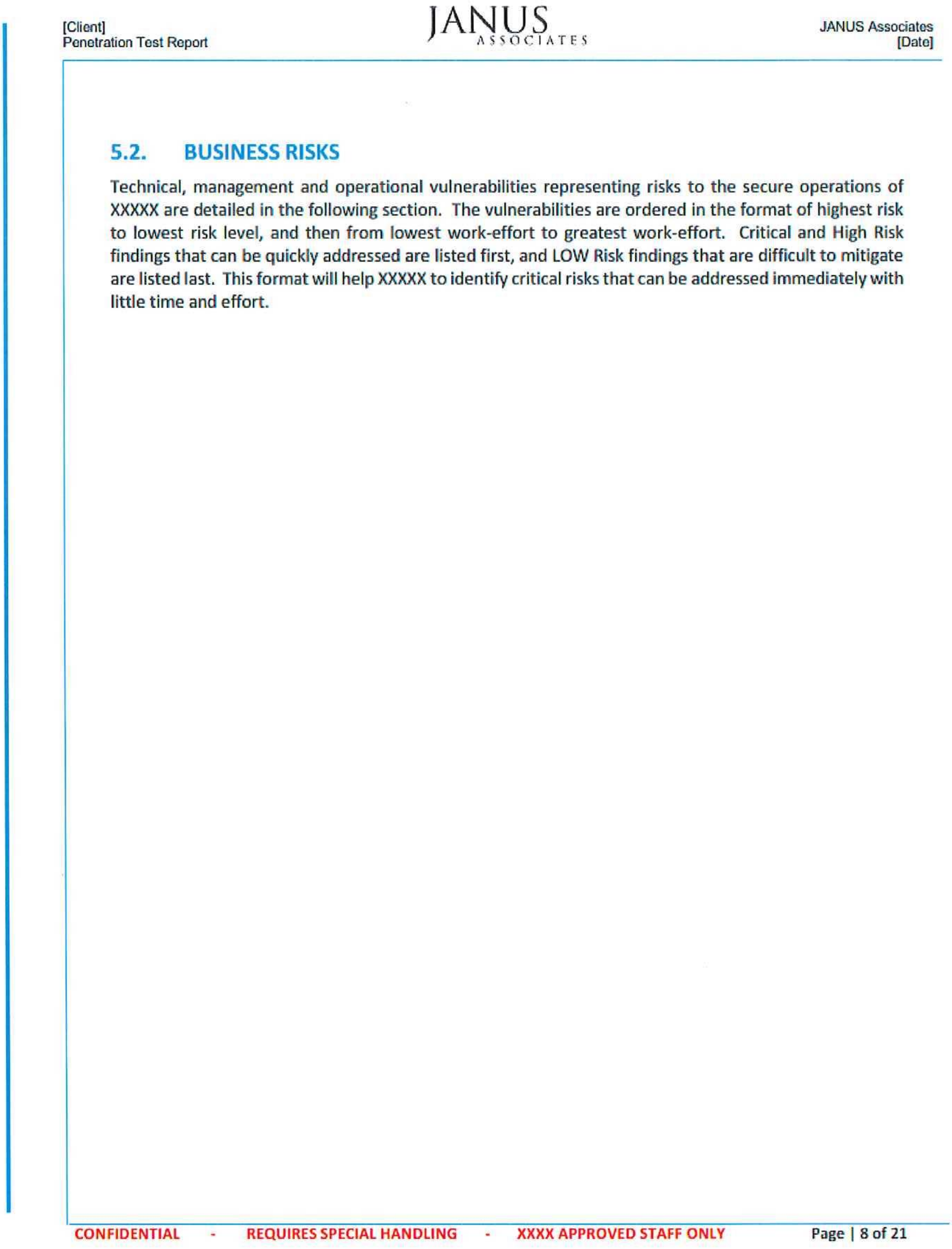


Rating	Definition of Ease-of-Fix Rating
	reliance on it. If it must be used, regular monitoring should be conducted to validate that security incidents have not occurred. **For other problems:** No known solution to the problem currently exists. Instead, all mitigating efforts to control the situation should be undertaken. It should be monitored to ensure that compromise has not occurred, and should be revisited annually to determine if a solution has been found.

5.1.3. ESTIMATED WORK EFFORT ASSESSMENT

Each Business Risk has been assigned an Estimated Work Effort value of Minimal, Moderate, Substantial or Unknown. The Estimated Work Effort value is an assessment of the extent of resources required to complete reasonable and appropriate corrective actions. The following definitions apply to the Estimated Work Effort values:

Rating	Definition of Estimated Work Effort Rating
Minimal	A limited investment of time (roughly three days or less) is required of a single individual to complete the corrective action(s).
Moderate	Time commitments of up to several weeks are required of multiple personnel.
Substantial	Significant time is required of multiple personnel to complete the corrective action(s). Examples of substantial work efforts include the redesign and implementation of network architecture, and the implementation of new software with associated documentation, testing and training across multiple organizational units.
Unknown	The time necessary to reduce or eliminate the vulnerability is currently unknown.



[Client]
Penetration Test Report

JANUS
ASSOCIATES

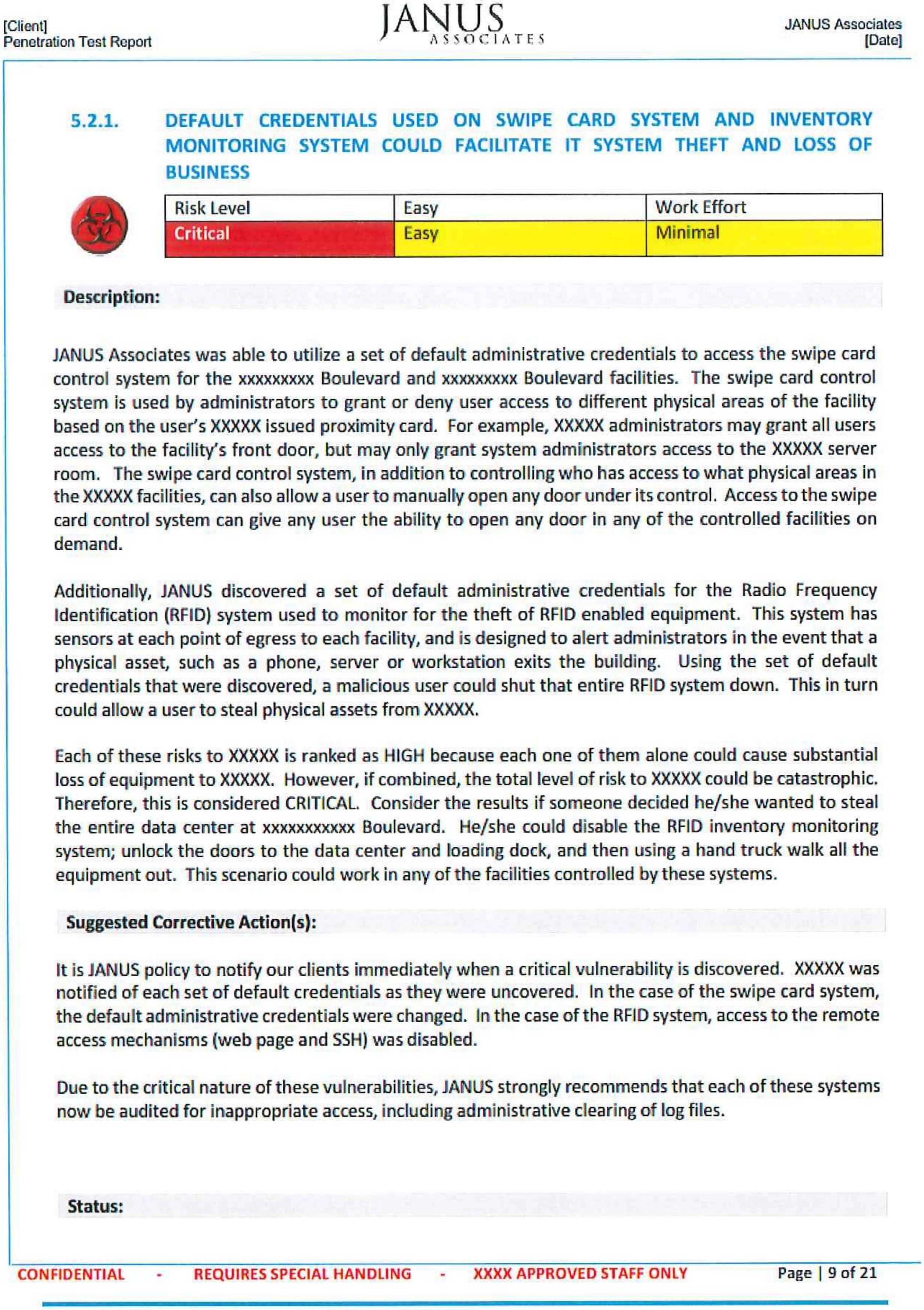
JANUS Associates
[Date]

5.2. BUSINESS RISKS

Technical, management and operational vulnerabilities representing risks to the secure operations of XXXXX are detailed in the following section. The vulnerabilities are ordered in the format of highest risk to lowest risk level, and then from lowest work-effort to greatest work-effort. Critical and High Risk findings that can be quickly addressed are listed first, and LOW Risk findings that are difficult to mitigate are listed last. This format will help XXXXX to identify critical risks that can be addressed immediately with little time and effort.

CONFIDENTIAL - REQUIRES SPECIAL HANDLING - XXXX APPROVED STAFF ONLY

Page | 8 of 21



5.2.1. DEFAULT CREDENTIALS USED ON SWIPE CARD SYSTEM AND INVENTORY MONITORING SYSTEM COULD FACILITATE IT SYSTEM THEFT AND LOSS OF BUSINESS

Risk Level	Easy	Work Effort
Critical	Easy	Minimal

Description:

JANUS Associates was able to utilize a set of default administrative credentials to access the swipe card control system for the xxxxxxxxx Boulevard and xxxxxxxxx Boulevard facilities. The swipe card control system is used by administrators to grant or deny user access to different physical areas of the facility based on the user's XXXXX issued proximity card. For example, XXXXX administrators may grant all users access to the facility's front door, but may only grant system administrators access to the XXXXX server room. The swipe card control system, in addition to controlling who has access to what physical areas in the XXXXX facilities, can also allow a user to manually open any door under its control. Access to the swipe card control system can give any user the ability to open any door in any of the controlled facilities on demand.

Additionally, JANUS discovered a set of default administrative credentials for the Radio Frequency Identification (RFID) system used to monitor for the theft of RFID enabled equipment. This system has sensors at each point of egress to each facility, and is designed to alert administrators in the event that a physical asset, such as a phone, server or workstation exits the building. Using the set of default credentials that were discovered, a malicious user could shut that entire RFID system down. This in turn could allow a user to steal physical assets from XXXXX.

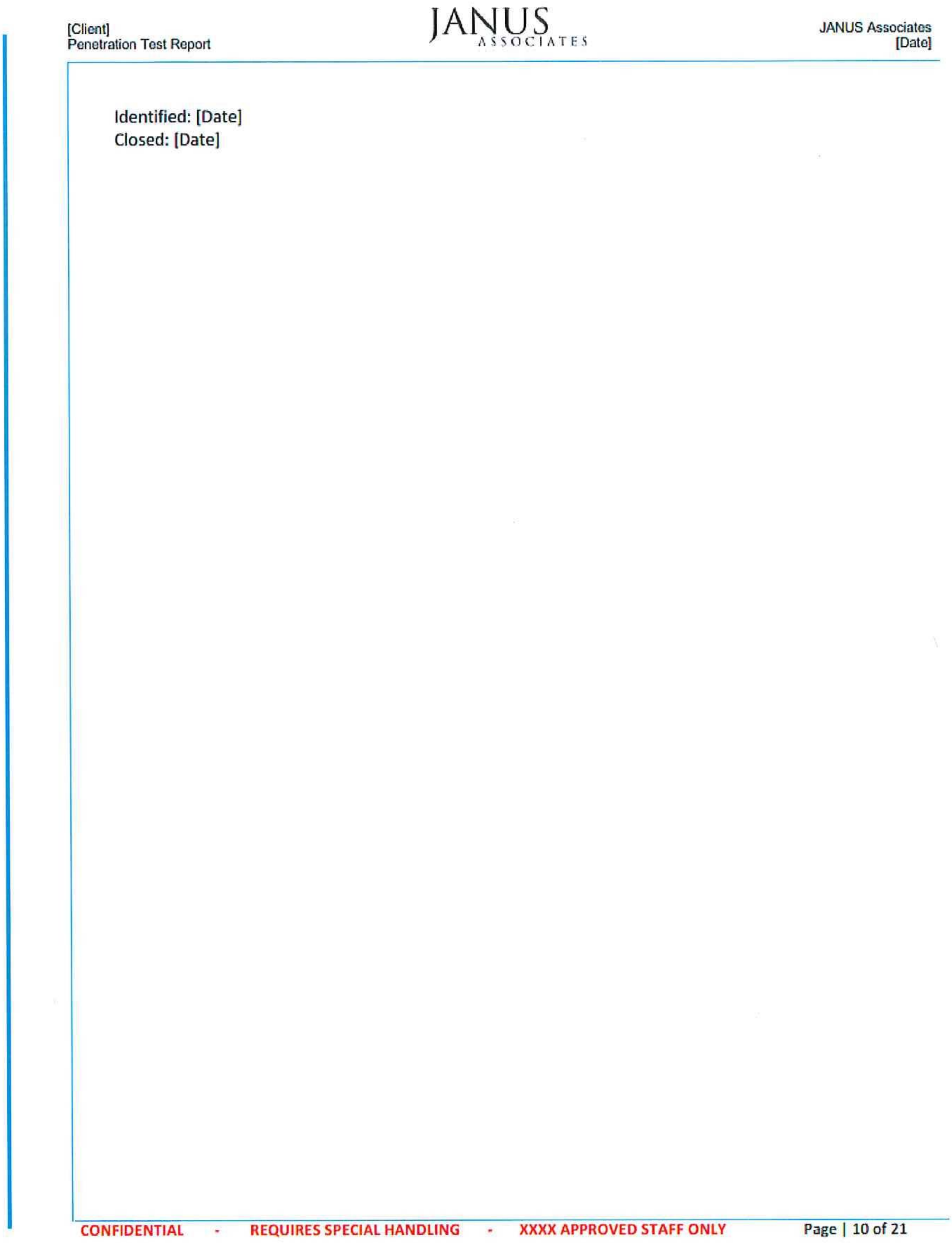
Each of these risks to XXXXX is ranked as HIGH because each one of them alone could cause substantial loss of equipment to XXXXX. However, if combined, the total level of risk to XXXXX could be catastrophic. Therefore, this is considered CRITICAL. Consider the results if someone decided he/she wanted to steal the entire data center at xxxxxxxxxxx Boulevard. He/she could disable the RFID inventory monitoring system; unlock the doors to the data center and loading dock, and then using a hand truck walk all the equipment out. This scenario could work in any of the facilities controlled by these systems.

Suggested Corrective Action(s):

It is JANUS policy to notify our clients immediately when a critical vulnerability is discovered. XXXXX was notified of each set of default credentials as they were uncovered. In the case of the swipe card system, the default administrative credentials were changed. In the case of the RFID system, access to the remote access mechanisms (web page and SSH) was disabled.

Due to the critical nature of these vulnerabilities, JANUS strongly recommends that each of these systems now be audited for inappropriate access, including administrative clearing of log files.

Status:



Identified: [Date]
Closed: [Date]

5.2.2. ABILITY TO ACCESS SERVER POWER OFF AND CONSOLE FEATURES GIVES AN ATTACKER ABILITY TO DISRUPT CRITICAL BUSINESS PROCESSES

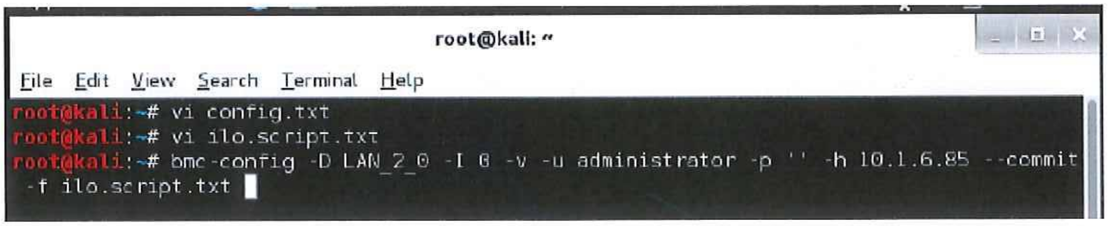
Risk Level	Ease-of-Fix	Work Effort
High	**Moderately Difficult**	**Moderate**

Description:

The server XXXXXSQLDBPRO05 is susceptible to a well-known vulnerability which allows an attacker to connect to the Intelligent Platform Management Interface (IPMI) console over the network. This attack is made possible by a flaw in the IPMI protocol. As a result, anyone with access to the network could create an administrative user on the system and physically shut down the system.

REDACTED

By using the command detailed in the following graphic an administrative user was created within the system.



```
root@kali:~# vi config.txt
root@kali:~# vi ilo.script.txt
root@kali:~# bmc-config -D LAN_2_0 -I 0 -v -u administrator -p '' -h 10.1.6.85 --commit
 -f ilo.script.txt
```

Below, we see the result of issuing the IPMI configuration.

REDACTED

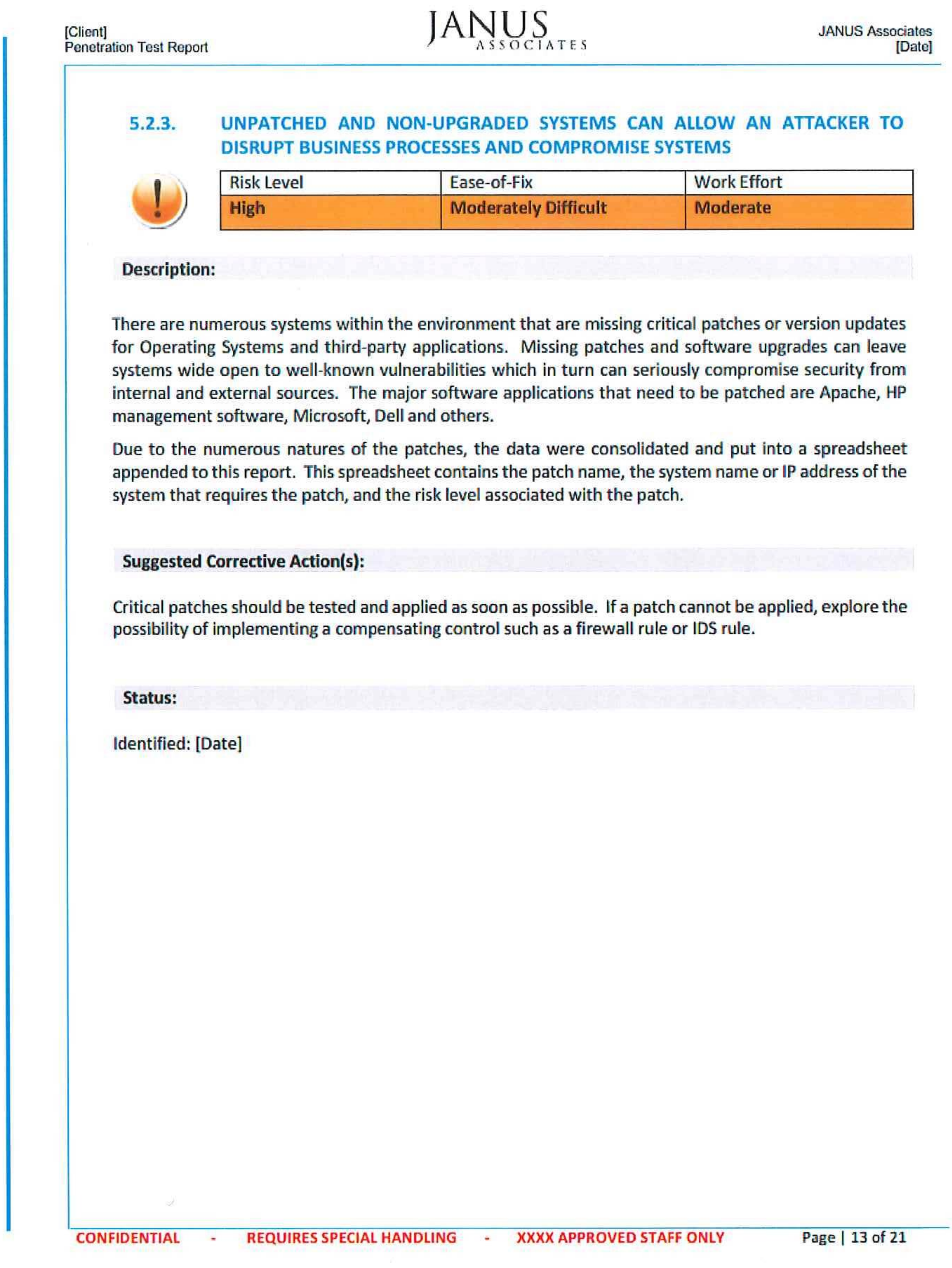
Once the new administrative user is created the username and password supplied can be used to access the administrative interface of the server.

Suggested Corrective Action(s):

1) Remove the "JANUSUser" account from the IPMI interface. This account was created to confirm the vulnerability.
2) If possible, patch the IPMI service. If a patch is not available, or cannot be applied,
    a. Uninstall the IPMI service.
    b. Restrict access to the service via a firewall.

Status:

Identified: [Date]



5.2.3. UNPATCHED AND NON-UPGRADED SYSTEMS CAN ALLOW AN ATTACKER TO DISRUPT BUSINESS PROCESSES AND COMPROMISE SYSTEMS

Risk Level	Ease-of-Fix	Work Effort
High	**Moderately Difficult**	**Moderate**

Description:

There are numerous systems within the environment that are missing critical patches or version updates for Operating Systems and third-party applications. Missing patches and software upgrades can leave systems wide open to well-known vulnerabilities which in turn can seriously compromise security from internal and external sources. The major software applications that need to be patched are Apache, HP management software, Microsoft, Dell and others.

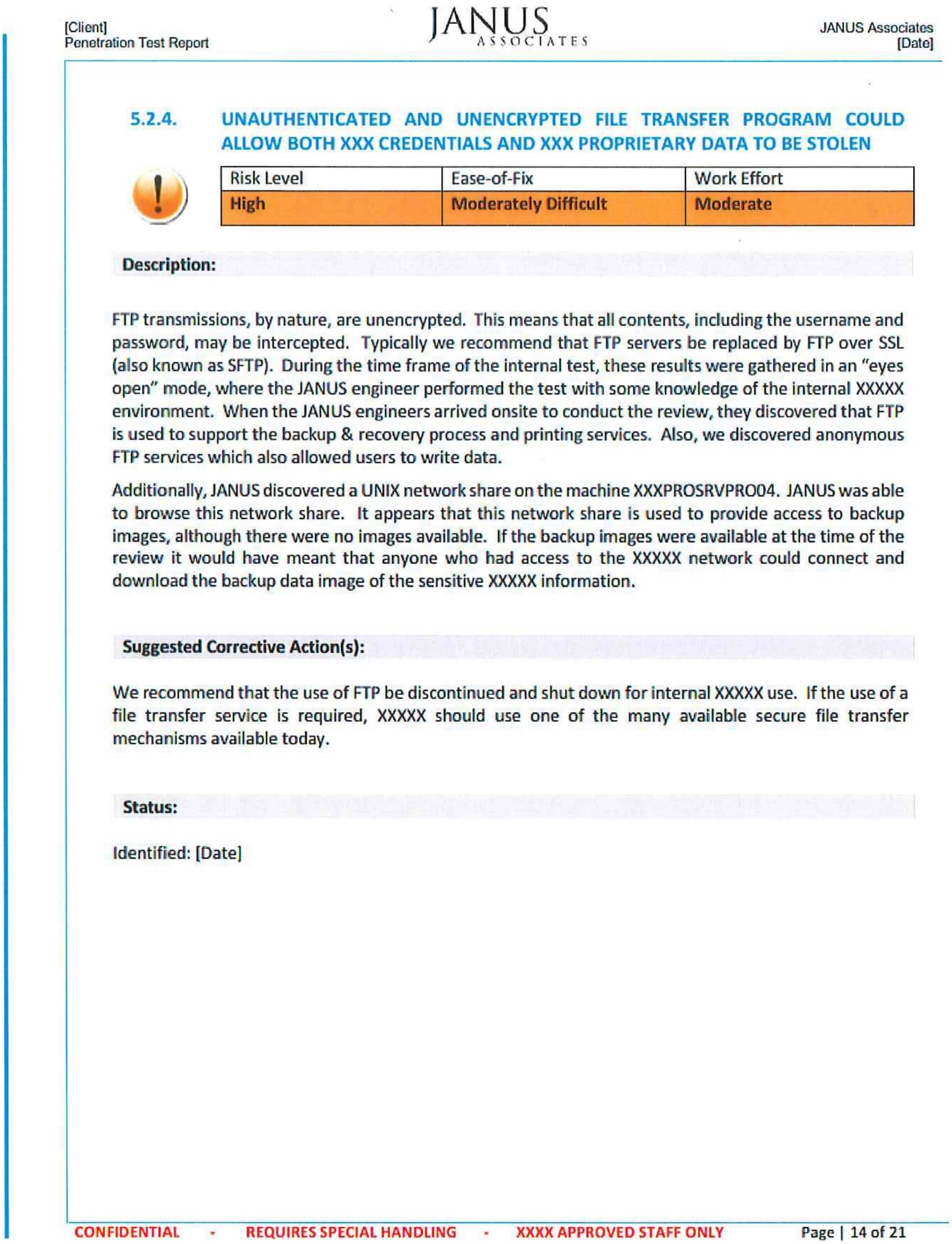
Due to the numerous natures of the patches, the data were consolidated and put into a spreadsheet appended to this report. This spreadsheet contains the patch name, the system name or IP address of the system that requires the patch, and the risk level associated with the patch.

Suggested Corrective Action(s):

Critical patches should be tested and applied as soon as possible. If a patch cannot be applied, explore the possibility of implementing a compensating control such as a firewall rule or IDS rule.

Status:

Identified: [Date]



5.2.4. UNAUTHENTICATED AND UNENCRYPTED FILE TRANSFER PROGRAM COULD ALLOW BOTH XXX CREDENTIALS AND XXX PROPRIETARY DATA TO BE STOLEN

Risk Level	Ease-of-Fix	Work Effort
High	**Moderately Difficult**	**Moderate**

Description:

FTP transmissions, by nature, are unencrypted. This means that all contents, including the username and password, may be intercepted. Typically we recommend that FTP servers be replaced by FTP over SSL (also known as SFTP). During the time frame of the internal test, these results were gathered in an "eyes open" mode, where the JANUS engineer performed the test with some knowledge of the internal XXXXX environment. When the JANUS engineers arrived onsite to conduct the review, they discovered that FTP is used to support the backup & recovery process and printing services. Also, we discovered anonymous FTP services which also allowed users to write data.

Additionally, JANUS discovered a UNIX network share on the machine XXXPROSRVPRO04. JANUS was able to browse this network share. It appears that this network share is used to provide access to backup images, although there were no images available. If the backup images were available at the time of the review it would have meant that anyone who had access to the XXXXX network could connect and download the backup data image of the sensitive XXXXX information.

Suggested Corrective Action(s):

We recommend that the use of FTP be discontinued and shut down for internal XXXXX use. If the use of a file transfer service is required, XXXXX should use one of the many available secure file transfer mechanisms available today.

Status:

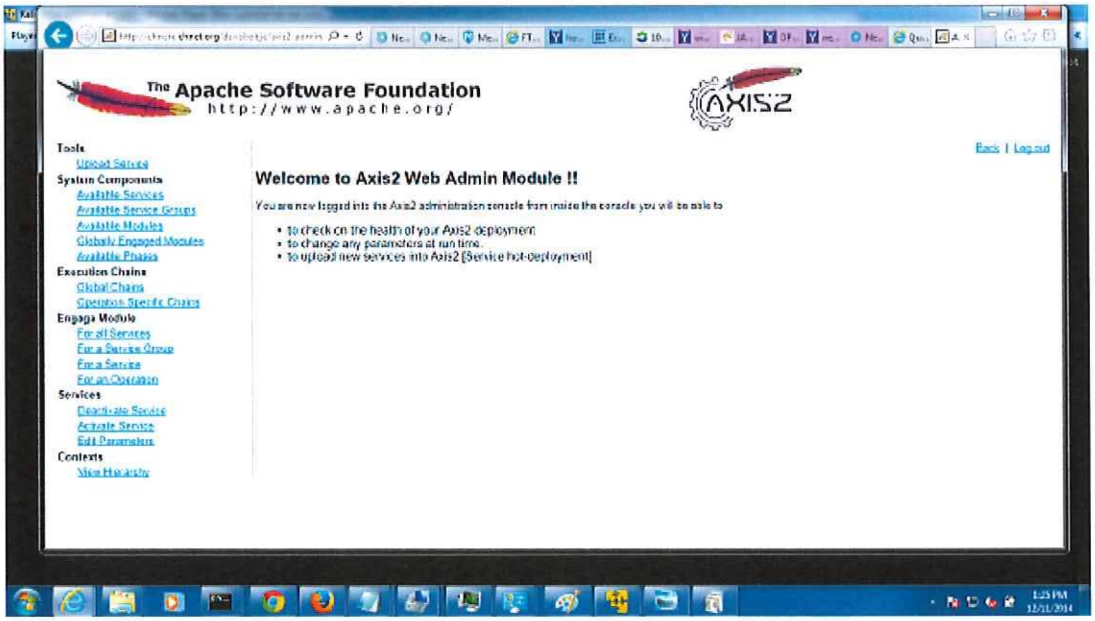
Identified: [Date]

5.2.5. DEFAULT CREDENTIALS AND KNOWN VULNERABILITIES ON XXX.COM COULD ALLOW AN ATTACKER TO DISRUPT THE SYSTEM AND MAKE IT UNAVAILABLE.

Risk Level	Ease-of-Fix	Work Effort
High	**Moderately Difficult**	**Moderate**

Description:

The Apache Axis 2 Installation on XXXXXCRE.XXXXX.COM still has a set of default credentials enabled. By having the default credentials enabled any user can log in and administer or configure the system. Additionally, there is a known Cross Site Scripting (XSS) flaw in this Apache installation, which could allow an attacker to inject client-side script into Web pages viewed by other users.



Welcome to Axis2 Web Admin Module !!

You are now logged into the Axis2 administration console from inside the console you will be able to

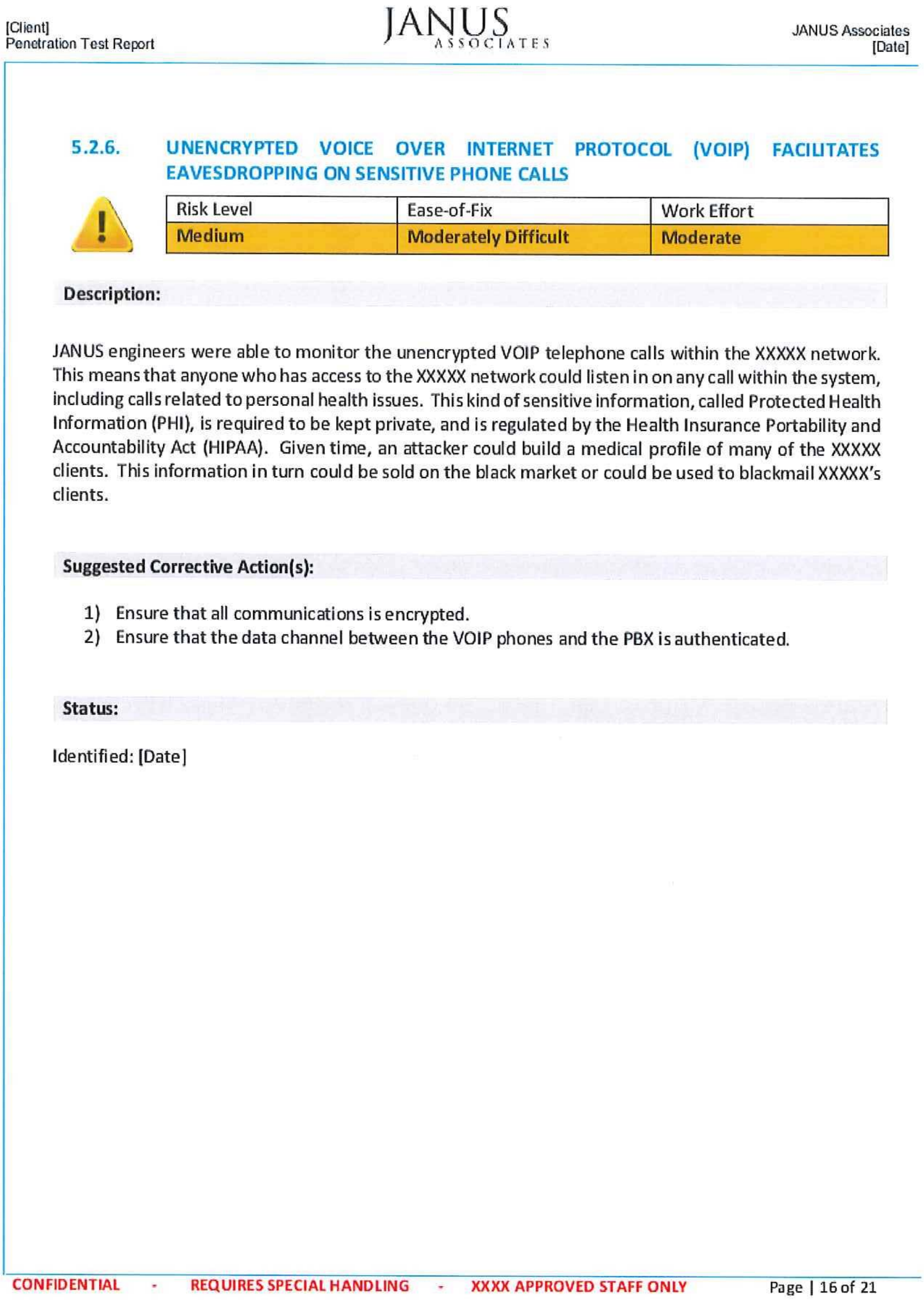
- to check on the health of your Axis2 deployment
- to change any parameters at run time.
- to upload new services into Axis2 [Service hot-deployment]

Suggested Corrective Action(s):

1) Determine if the Apache Axis installation is required. If it is not, uninstall or disable it.
2) If the Apache Axis installation is required, patch it to the most recent version and change the default password.

Status:

Identified: [Date]



[Client]
Penetration Test Report

JANUS
ASSOCIATES

JANUS Associates
[Date]

5.2.6. UNENCRYPTED VOICE OVER INTERNET PROTOCOL (VOIP) FACILITATES EAVESDROPPING ON SENSITIVE PHONE CALLS

Risk Level	Ease-of-Fix	Work Effort
Medium	Moderately Difficult	Moderate

Description:

JANUS engineers were able to monitor the unencrypted VOIP telephone calls within the XXXXX network. This means that anyone who has access to the XXXXX network could listen in on any call within the system, including calls related to personal health issues. This kind of sensitive information, called Protected Health Information (PHI), is required to be kept private, and is regulated by the Health Insurance Portability and Accountability Act (HIPAA). Given time, an attacker could build a medical profile of many of the XXXXX clients. This information in turn could be sold on the black market or could be used to blackmail XXXXX's clients.

Suggested Corrective Action(s):

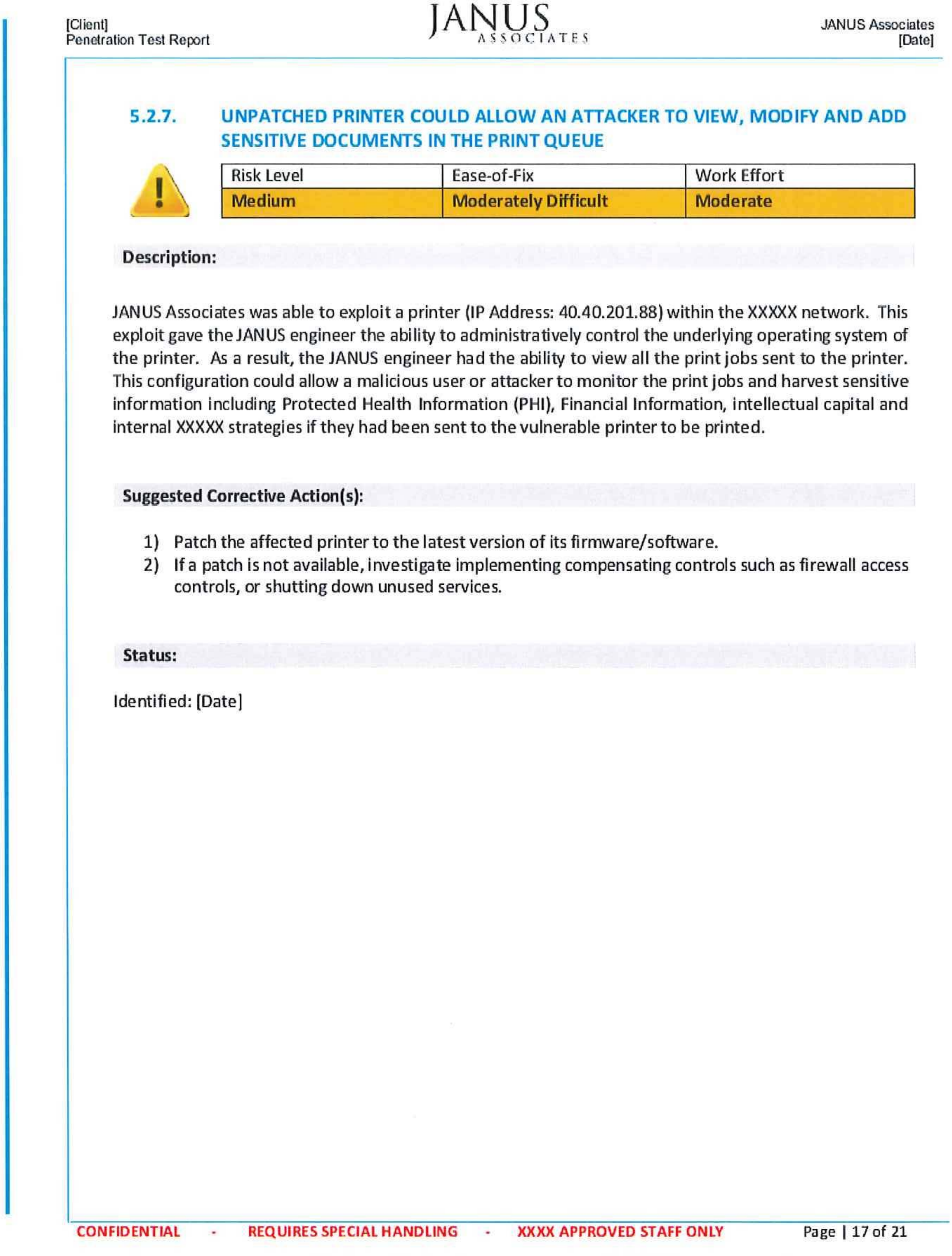
1) Ensure that all communications is encrypted.
2) Ensure that the data channel between the VOIP phones and the PBX is authenticated.

Status:

Identified: [Date]

CONFIDENTIAL - REQUIRES SPECIAL HANDLING - XXXX APPROVED STAFF ONLY

Page | 16 of 21



5.2.7. UNPATCHED PRINTER COULD ALLOW AN ATTACKER TO VIEW, MODIFY AND ADD SENSITIVE DOCUMENTS IN THE PRINT QUEUE

Risk Level	Ease-of-Fix	Work Effort
Medium	Moderately Difficult	Moderate

Description:

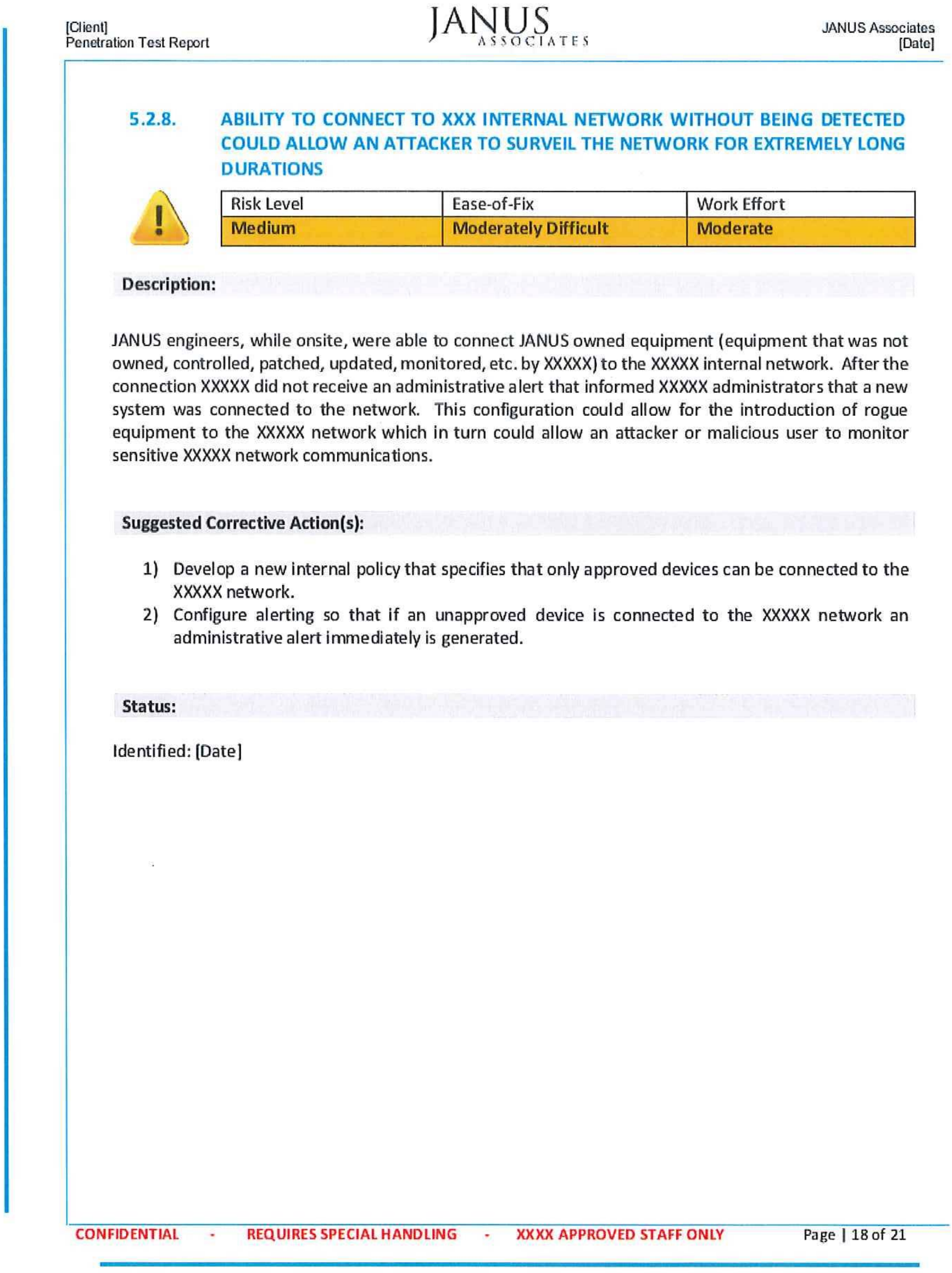
JANUS Associates was able to exploit a printer (IP Address: 40.40.201.88) within the XXXXX network. This exploit gave the JANUS engineer the ability to administratively control the underlying operating system of the printer. As a result, the JANUS engineer had the ability to view all the print jobs sent to the printer. This configuration could allow a malicious user or attacker to monitor the print jobs and harvest sensitive information including Protected Health Information (PHI), Financial Information, intellectual capital and internal XXXXX strategies if they had been sent to the vulnerable printer to be printed.

Suggested Corrective Action(s):

1) Patch the affected printer to the latest version of its firmware/software.
2) If a patch is not available, investigate implementing compensating controls such as firewall access controls, or shutting down unused services.

Status:

Identified: [Date]



5.2.8. ABILITY TO CONNECT TO XXX INTERNAL NETWORK WITHOUT BEING DETECTED COULD ALLOW AN ATTACKER TO SURVEIL THE NETWORK FOR EXTREMELY LONG DURATIONS

Risk Level	Ease-of-Fix	Work Effort
Medium	**Moderately Difficult**	**Moderate**

Description:

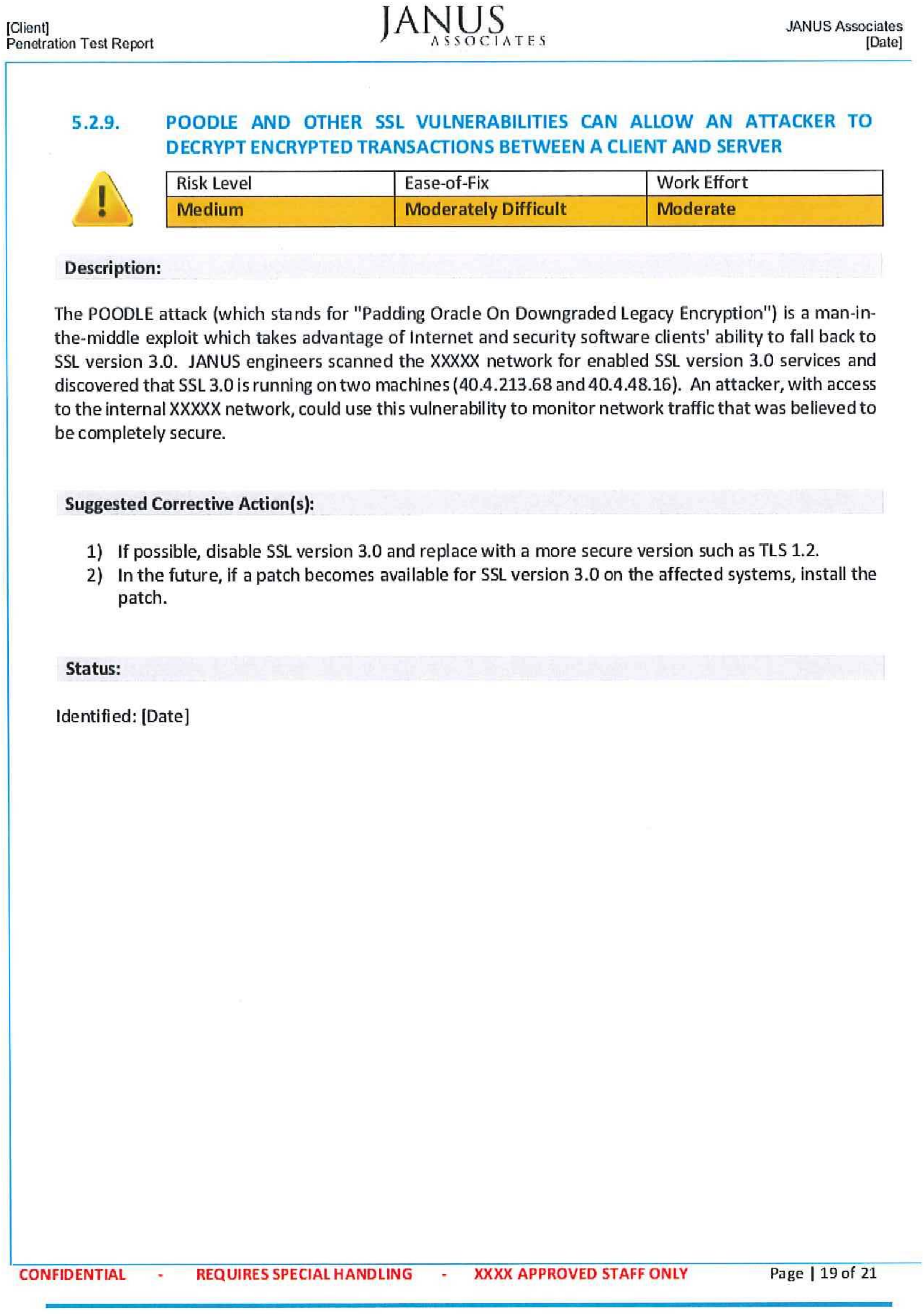
JANUS engineers, while onsite, were able to connect JANUS owned equipment (equipment that was not owned, controlled, patched, updated, monitored, etc. by XXXXX) to the XXXXX internal network. After the connection XXXXX did not receive an administrative alert that informed XXXXX administrators that a new system was connected to the network. This configuration could allow for the introduction of rogue equipment to the XXXXX network which in turn could allow an attacker or malicious user to monitor sensitive XXXXX network communications.

Suggested Corrective Action(s):

1) Develop a new internal policy that specifies that only approved devices can be connected to the XXXXX network.
2) Configure alerting so that if an unapproved device is connected to the XXXXX network an administrative alert immediately is generated.

Status:

Identified: [Date]



5.2.9. POODLE AND OTHER SSL VULNERABILITIES CAN ALLOW AN ATTACKER TO DECRYPT ENCRYPTED TRANSACTIONS BETWEEN A CLIENT AND SERVER

Risk Level	Ease-of-Fix	Work Effort
Medium	**Moderately Difficult**	**Moderate**

Description:

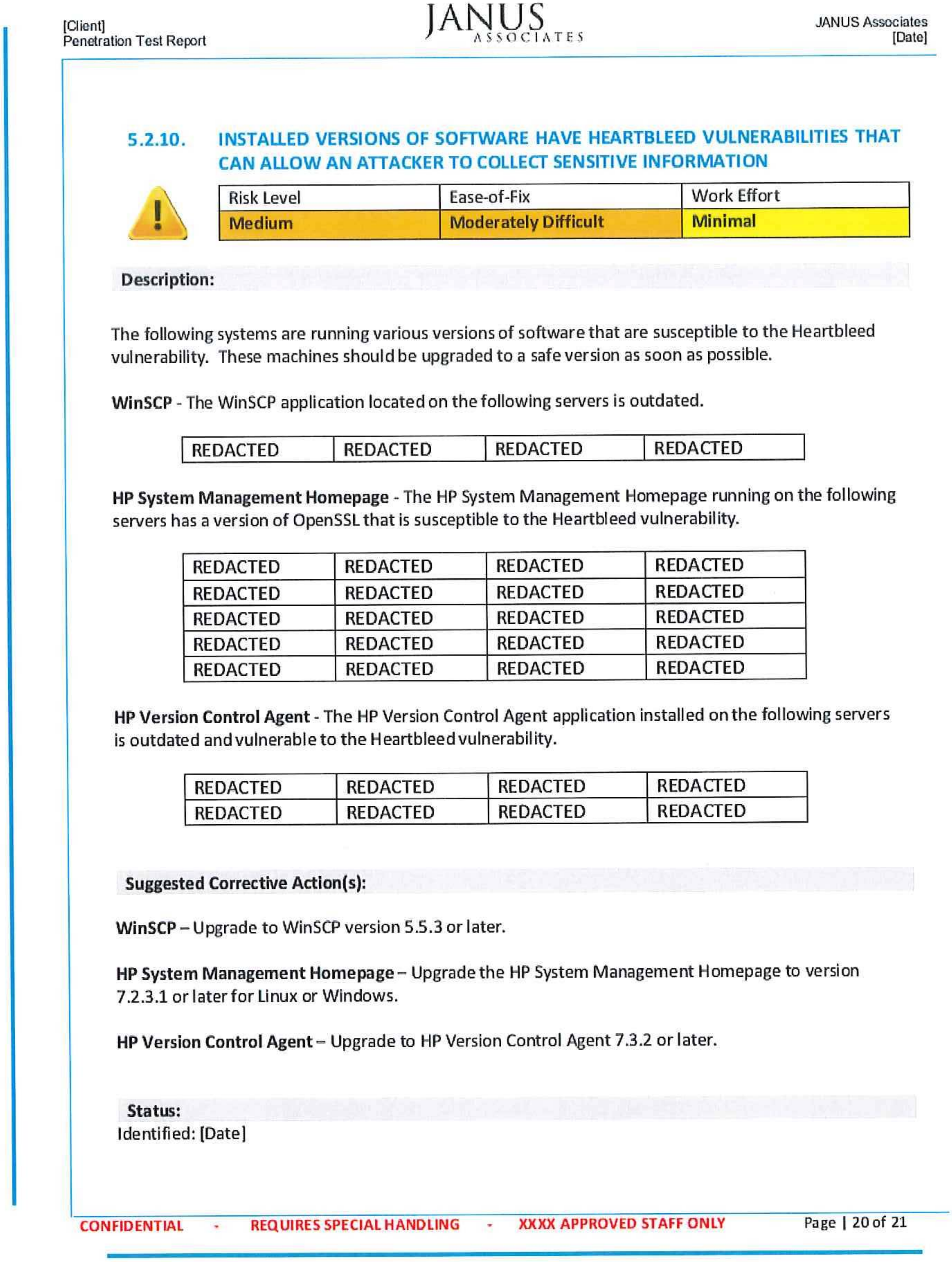
The POODLE attack (which stands for "Padding Oracle On Downgraded Legacy Encryption") is a man-in-the-middle exploit which takes advantage of Internet and security software clients' ability to fall back to SSL version 3.0. JANUS engineers scanned the XXXXX network for enabled SSL version 3.0 services and discovered that SSL 3.0 is running on two machines (40.4.213.68 and 40.4.48.16). An attacker, with access to the internal XXXXX network, could use this vulnerability to monitor network traffic that was believed to be completely secure.

Suggested Corrective Action(s):

1) If possible, disable SSL version 3.0 and replace with a more secure version such as TLS 1.2.
2) In the future, if a patch becomes available for SSL version 3.0 on the affected systems, install the patch.

Status:

Identified: [Date]



[Client]
Penetration Test Report

JANUS ASSOCIATES

JANUS Associates
[Date]

5.2.10. INSTALLED VERSIONS OF SOFTWARE HAVE HEARTBLEED VULNERABILITIES THAT CAN ALLOW AN ATTACKER TO COLLECT SENSITIVE INFORMATION

Risk Level	Ease-of-Fix	Work Effort
Medium	**Moderately Difficult**	**Minimal**

Description:

The following systems are running various versions of software that are susceptible to the Heartbleed vulnerability. These machines should be upgraded to a safe version as soon as possible.

WinSCP - The WinSCP application located on the following servers is outdated.

REDACTED	REDACTED	REDACTED	REDACTED

HP System Management Homepage - The HP System Management Homepage running on the following servers has a version of OpenSSL that is susceptible to the Heartbleed vulnerability.

REDACTED	REDACTED	REDACTED	REDACTED
REDACTED	REDACTED	REDACTED	REDACTED
REDACTED	REDACTED	REDACTED	REDACTED
REDACTED	REDACTED	REDACTED	REDACTED
REDACTED	REDACTED	REDACTED	REDACTED

HP Version Control Agent - The HP Version Control Agent application installed on the following servers is outdated and vulnerable to the Heartbleed vulnerability.

REDACTED	REDACTED	REDACTED	REDACTED
REDACTED	REDACTED	REDACTED	REDACTED

Suggested Corrective Action(s):

WinSCP – Upgrade to WinSCP version 5.5.3 or later.

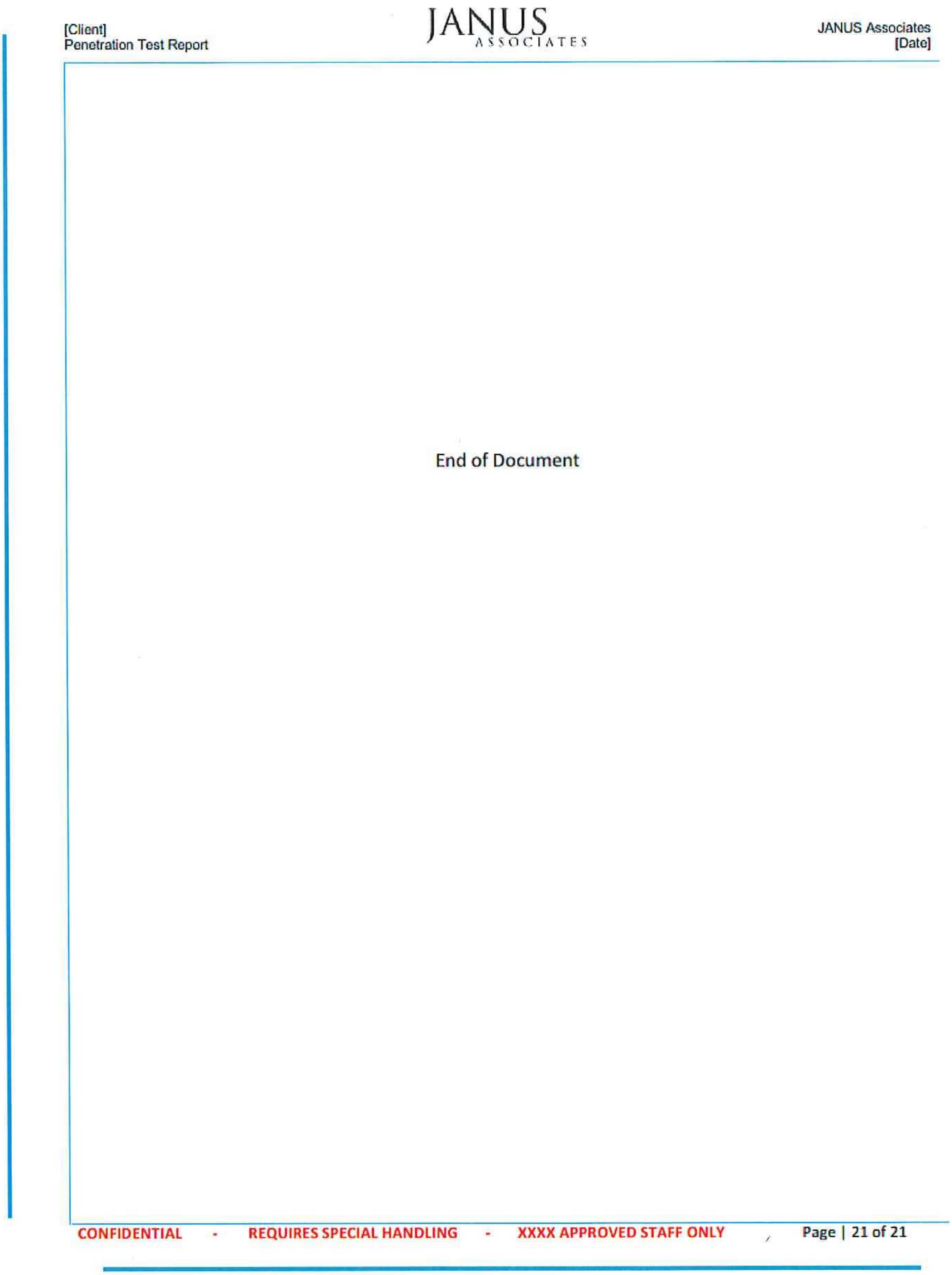
HP System Management Homepage – Upgrade the HP System Management Homepage to version 7.2.3.1 or later for Linux or Windows.

HP Version Control Agent – Upgrade to HP Version Control Agent 7.3.2 or later.

Status:
Identified: [Date]

CONFIDENTIAL - REQUIRES SPECIAL HANDLING - XXXX APPROVED STAFF ONLY

Page | 20 of 21



End of Document

Appendix C – Client Comments

State of Minnesota

From: Buse, Chris P (MNIT) [mailto:chris.buse@state.mn.us]
Sent: Wednesday, September 07, 2016 5:34 PM
To: Karl W. Muenzinger <karlm@janusassociates.com>; Dan Reed <DanR@JanusAssociates.COM>; Steve Zeve <SteveZ@JanusAssociates.COM>
Subject: Minnesota METS Audit Feedback

Karl, Dan and Steve,

I would like to start by introducing myself. My name is Christopher Buse and I am the CISO for the State of Minnesota. I also am a former auditor, who lead a technical audit function for many years.

I wanted to send your team a quick note to thank you for the outstanding work on the METS audit. I have been quite unimpressed with much of the IT audit work that has been done lately in our environment - and have got to the point where I have been setting the expectation bar pretty low. But your firm was a badly needed breath of fresh air. Chris Luhman – a very technical security leader on my team – provided me with some stellar feedback on the competency of your staff. He also was impressed by your team's ability to analyze results in relation to the full gamut of mitigating controls in the environment under inspection. This seems to be a lost art today, where many IT auditors call security tool outputs audit results, without proper verification or consideration of mitigating circumstances.

Though it would have been nice to have report with no high-risk findings, as the state's security leader I feel comfortable that the results are a true reflection of the security controls in our environment. And I also feel comfortable saying that I would definitely consider using your firm for security attest work down the road.

Nicely done, guys.

CHRISTOPHER BUSE CPA, CISSP, CISA | ASSISTANT COMMISSIONER AND CHIEF INFORMATION SECURITY OFFICER
MN.IT SERVICES, CENTRAL
651-201-1200 (w) | 651-356-1619 (m) | chris.buse@state.mn.us

MNIT SERVICES Information Technology for Minnesota Government | mn.gov/mnit

Maryland State Retirement Agency

From: David Toft [mailto:dtoft@sra.state.md.us]
Sent: Friday, March 11, 2016 3:58 PM
To: Karl W. Muenzinger <karlm@janusassociates.com>
Subject: RE: MSRA Penetration test and Code Review

Karl – IS management just had a debriefing on the Janus engagement this morning.

We accept the two reports as final and no further changes are necessary. The signed acceptance forms are attached.

Our goal is to run our Agency operations as securely as possible and your professional IT team have helped us in that regard.

Thank you and for your staff for a successful security assessment and for the valued input Janus has provided us.

Best Regards,
David

David S. Toft, Sr., CISSP
Dir. Information Systems Data Security & Quality
Maryland State Retirement and Pension System
120 East Baltimore Street | Baltimore, MD | 21202-6700
Tel: 410-625-5562 | 1-800-492-5909 | TDD/TTY 410-625-5535
sra.maryland.gov

Anonymous

From: Gxxxxxxx [mailto:gxxxxxx@xxxxx.com]
Sent: Friday, December 16, 2016 12:20 PM
To: Adam Fisher <AdamF@JanusAssociates.COM>
Subject: RE: Social Engineering

Great work. These employees just finished the cyber awareness training and phishing was covered in detail so they should have known better, just goes to show you cannot stop 100%.

Thanks,
Gxxxx

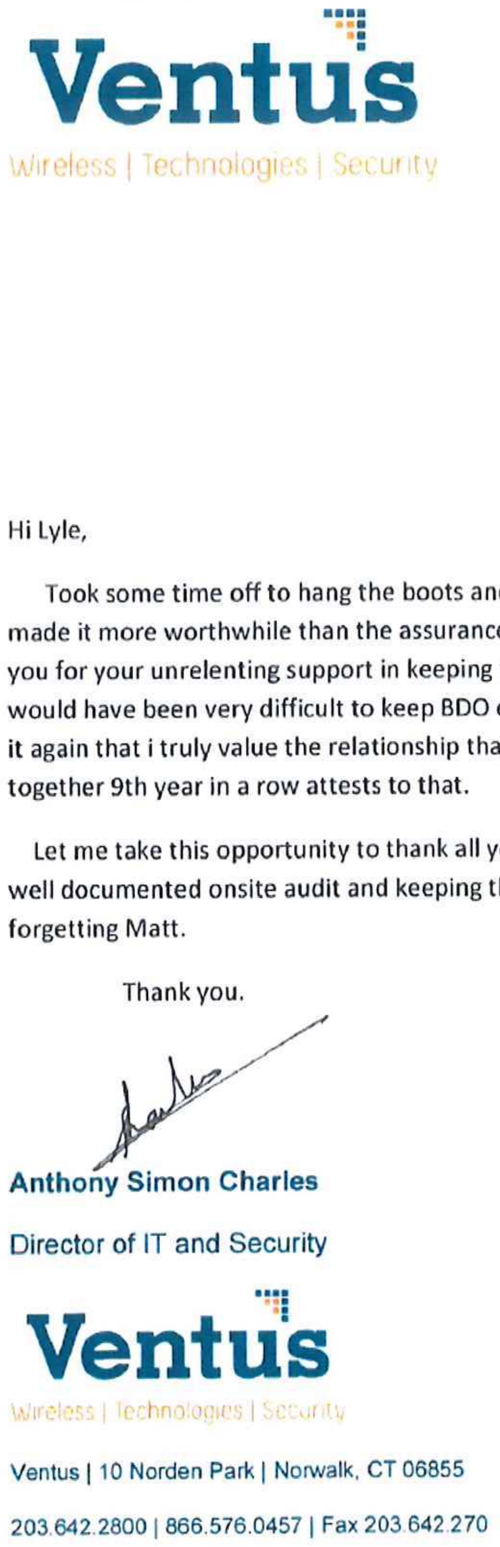
From: Adam Fisher [mailto:AdamF@JanusAssociates.COM]
Sent: Friday, December 16, 2016 12:13 PM
To: Gxxxxxxx <gxxxxxx@xxxxx.com>
Subject: RE: Social Engineering

OK, then I'm stopping. I'm into Citrix currently.

Adam G. Fisher
JANUS Associates, Inc.
1.203.251.0169 (w)
1.617.872.6486 (c)
1.203.251.0222 (f)
http://www.janusassociates.com

This e-mail and any files transmitted with it are the property of JANUS Associates, Inc., are confidential and, are intended solely for the use of the individual or entity to whom this e-mail is addressed. If you are not one of the named recipient(s) or otherwise have reason to believe that you have received this message in error, please notify the sender at 203-251-0200 and delete this message immediately from your computer. Do not divulge, copy, forward, or use the contents, attachments, or information without permission of JANUS Associates, Inc. Any other use, retention, dissemination, forwarding, printing, or copying of this e-mail is strictly prohibited.

Ventus (September 2015)



Ventus

Wireless | Technologies | Security

Hi Lyle,

Took some time off to hang the boots and play with my little (now 1 year old) daughter. Nothing made it more worthwhile than the assurance that we have the ROC in hand. Let me personally thank you for your unrelenting support in keeping the effort alive. Without your intervention and persuasion it would have been very difficult to keep BDO engaged and committed. I have said that in the past and say it again that i truly value the relationship that we have with Janus and the fact that we continue to work together 9th year in a row attests to that.

Let me take this opportunity to thank all your team members especially George for his key role in the well documented onsite audit and keeping the BDO technical team engaged and aligned, while not forgetting Matt.

Thank you.

Anthony Simon Charles

Director of IT and Security

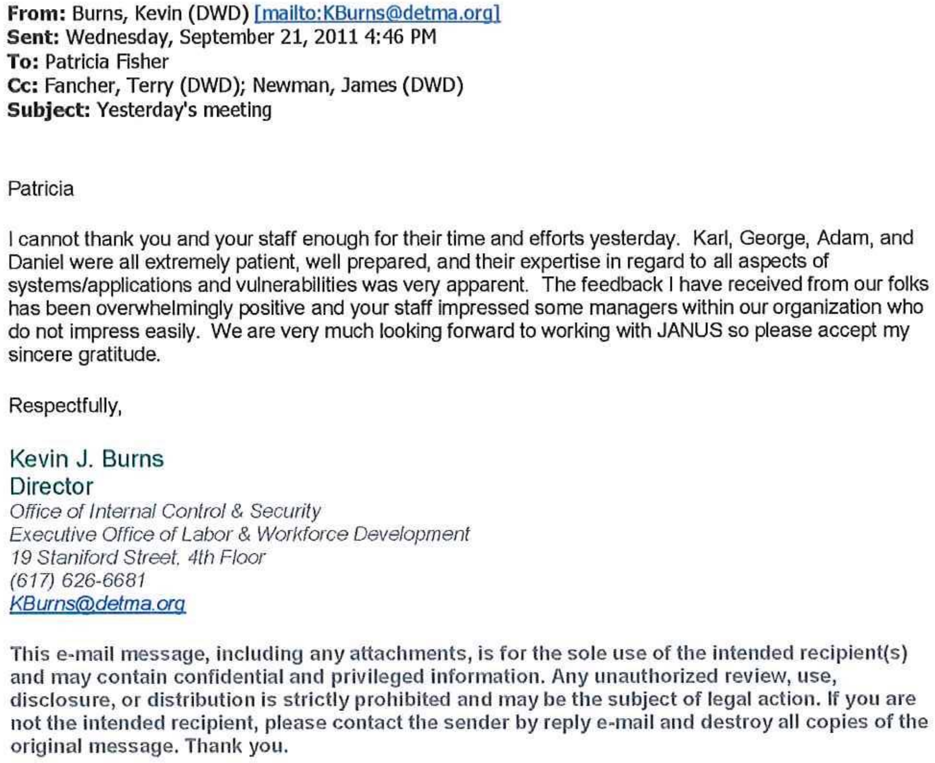
Ventus

Wireless | Technologies | Security

Ventus | 10 Norden Park | Norwalk, CT 06855

203.642.2800 | 866.576.0457 | Fax 203.642.270

Commonwealth of Massachusetts Department of Labor and Workforce Development



From: Burns, Kevin (DWD) [mailto:KBurns@detma.org]
Sent: Wednesday, September 21, 2011 4:46 PM
To: Patricia Fisher
Cc: Fancher, Terry (DWD); Newman, James (DWD)
Subject: Yesterday's meeting

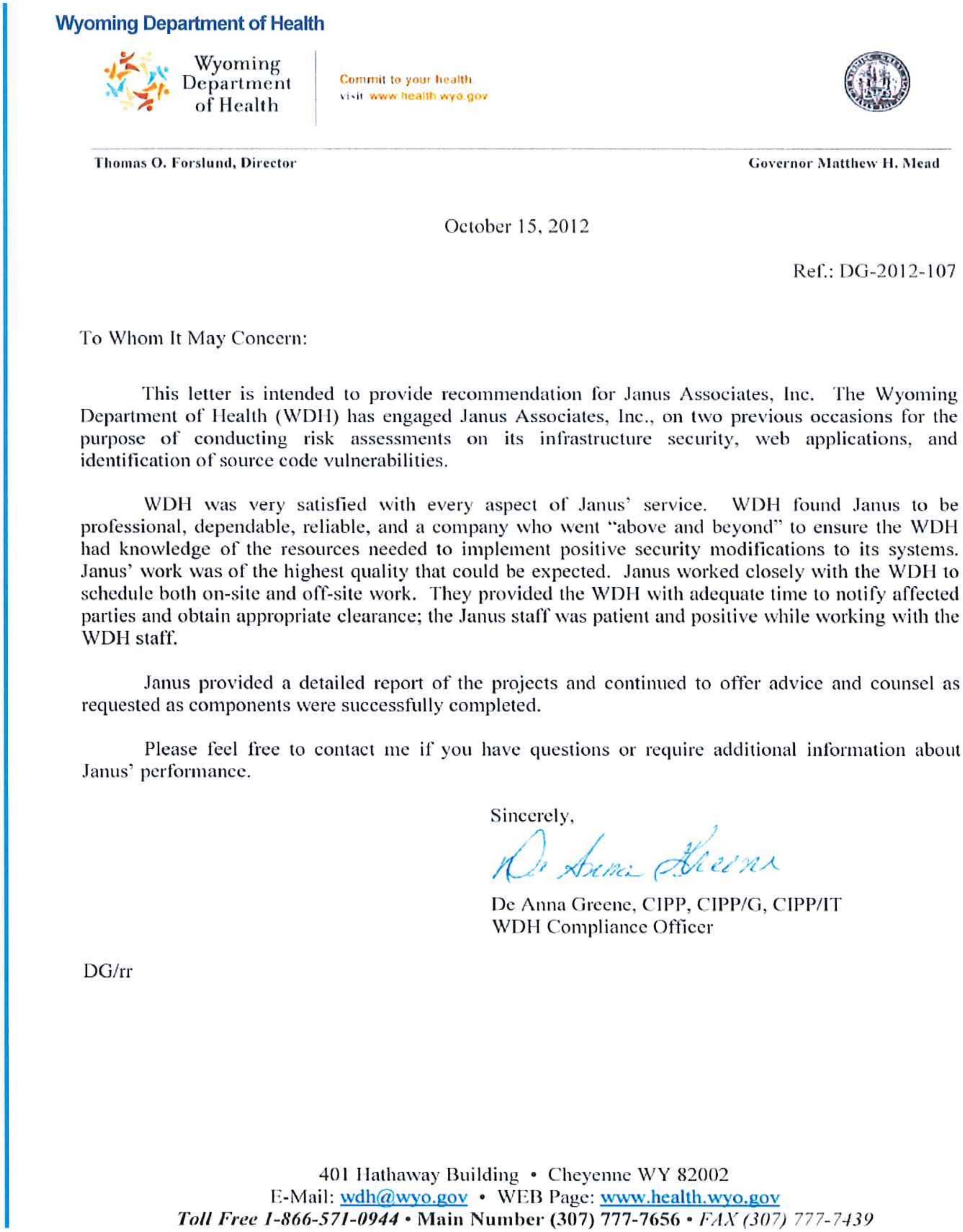
Patricia

I cannot thank you and your staff enough for their time and efforts yesterday. Karl, George, Adam, and Daniel were all extremely patient, well prepared, and their expertise in regard to all aspects of systems/applications and vulnerabilities was very apparent. The feedback I have received from our folks has been overwhelmingly positive and your staff impressed some managers within our organization who do not impress easily. We are very much looking forward to working with JANUS so please accept my sincere gratitude.

Respectfully,

Kevin J. Burns
Director
Office of Internal Control & Security
Executive Office of Labor & Workforce Development
19 Staniford Street, 4th Floor
(617) 626-6681
KBurns@detma.org

This e-mail message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized review, use, disclosure, or distribution is strictly prohibited and may be the subject of legal action. If you are not the intended recipient, please contact the sender by reply e-mail and destroy all copies of the original message. Thank you.



Wyoming Department of Health

Wyoming
Department
of Health

Commit to your health
visit www.health.wyo.gov

Thomas O. Forslund, Director

Governor Matthew H. Mead

October 15, 2012

Ref.: DG-2012-107

To Whom It May Concern:

This letter is intended to provide recommendation for Janus Associates, Inc. The Wyoming Department of Health (WDH) has engaged Janus Associates, Inc., on two previous occasions for the purpose of conducting risk assessments on its infrastructure security, web applications, and identification of source code vulnerabilities.

WDH was very satisfied with every aspect of Janus' service. WDH found Janus to be professional, dependable, reliable, and a company who went "above and beyond" to ensure the WDH had knowledge of the resources needed to implement positive security modifications to its systems. Janus' work was of the highest quality that could be expected. Janus worked closely with the WDH to schedule both on-site and off-site work. They provided the WDH with adequate time to notify affected parties and obtain appropriate clearance; the Janus staff was patient and positive while working with the WDH staff.

Janus provided a detailed report of the projects and continued to offer advice and counsel as requested as components were successfully completed.

Please feel free to contact me if you have questions or require additional information about Janus' performance.

Sincerely,

De Anna Greene

De Anna Greene, CIPP, CIPP/G, CIPP/IT
WDH Compliance Officer

DG/rr

401 Hathaway Building • Cheyenne WY 82002
E-Mail: wdh@wyo.gov • WEB Page: www.health.wyo.gov
Toll Free 1-866-571-0944 • **Main Number (307) 777-7656** • *FAX (307) 777-7439*

End of Document

Cyber Security

RFP # 5905

Proposal
Prepared for:
City of Hartford

SEAL OF THE CITY OF HARTFORD
POST NUBILA PHOEBUS
CONNECTICUT

April 5, 2019

COPY

JANUS
ASSOCIATES

CELEBRATING
30 YEARS
PROTECTING
client data since 1988

Prepared by:
JANUS Software, Inc.
d/b/a JANUS Associates
4 High Ridge Park
Stamford, CT 06905
Contact: Patricia Fisher
patfisher@janusassociates.com

Table of Contents

JANUS
ASSOCIATES

April 5, 2019

Mr. William Diaz
Procurement Specialist
Procurement Services Unit
City of Hartford
550 Main Street, Suite 100
Hartford, CT 06103

Dear Mr. Diaz:

JANUS Software, Inc., d/b/a JANUS Associates (JANUS) is pleased to present the City of Hartford, Connecticut (City), Metro Hartford Innovation Services (MHIS) with this proposal for Cyber Security Consulting Services.

Since being founded in 1988, JANUS has had its core competency providing leading edge information security services and has extensive experience in performing the types of security services requested by the City. We regularly provide similar services for federal, state and local government entities, private sector businesses, higher education, and not-for-profit organizations. Examples of recent similar projects include the Schertz-Cibolo-Universal City Independent School District of San Antonio, Texas; Commonwealth of Pennsylvania; Madison County, Illinois government; University of Central Arkansas; and New York City, amongst many others.

Over our entire history, we have built a well-deserved reputation for high quality, "on time, within budget" performance and for consistently high client satisfaction. These attributes are due to the skills and professionalism of JANUS staff and to our firm's dedication to delivering quality services in complex environments, providing leading edge experience and true value for clients – while remaining free of any vendor affiliations. As a result, our recommendations are totally focused on your needs, and are not associated with selling tools, or vendor offerings.

You may very well receive lower cost proposals. However, in cyber security, these low-cost alternatives come with their own price – which is lack of skill – and skill is the key element in cyber security services which can assist you in avoiding breaches and attacks. In addition, our clients report to us that these lower priced alternatives always result in higher costs because work is left undone which our client must then figure out and complete. With JANUS, you will not receive a more thorough assessments or stronger IT security services at a fair price designed to protect your assets than those offered by JANUS. We have also been informed by our clients that we offer more detailed (and thorough) analysis in our assessments and consulting. We are passionate about doing the right thing for you and protecting your environment at the level needed.

Thank you for allowing JANUS the opportunity to submit this proposal. We are ready to begin this project, and JANUS management and staff look forward to working with your team to meet your security goals and objectives and to exceed expectations as a service provider.

Sincerely,

Patricia A. P. Fisher

Patricia A. P. Fisher
President & CEO

SECTION 1 – RESPONSE FORMS

Section 1
RESPONSE FORMS

1.1 RESPONSE INFORMATION & SIGNATURE FORM

Vendor Name - JANUS Software, Inc. (d/b/a JANUS Associates)				
Trade Name - N/A				
Address - 4 High Ridge Park, Stamford, CT 06905				
Phone # - 203-251-0200	**Fax # - 203-251-0222**	**Email Address - patfisher@janusassociates.com**		
Contact Person - Patricia A. P. Fisher		**Tax ID# - 59-3026157**		
Delivery / Service Start Date: TBD		# Calendar days after receipt of executed contract: 14		
Bid Surety - 10%	For electronic bonds enter bond number, otherwise check the appropriate box	Electronic Bond # N/A	□ Bond (hard copy) N/A	□ Cashiers / Certified Check N/A
Cost of Performance Bond included in base bid (if applicable)			$N/A	Per thousand
EEO Certification Status (check one) See General Information for Preparing a Response paragraph 3.6.3			□ Current & on file	☒ EEO form attached
DAS Prequalified Contractor? (non-highway construction projects >$500,000) http://das.ct.gov/cr1.aspx?page=10			□ Certificate attached N/A	□ Update Statement attached N/A
Insurance Agent Name	Ferguson & McGuire, Inc.		Phone #203-269-9565	
Insurance Agent Address	6 North Main Street, P.O. Box 846, Wallingford, CT 06492			

Vendor acknowledges receipt of all addenda issued during the bidding period (if applicable) and understands that they are a part of the bidding documents.

The undersigned hereby declares that he/she or they are thoroughly familiar with the specifications, the various sites, the City's requirements, and the objectives for each element of the project item or service and understands that in signing this proposal all right to plead any misunderstanding regarding the same is waived. The undersigned further understands and agrees that he will furnish and provide all the necessary material, machinery, implements, tools, labor, services, and other items of whatever nature, and to do and perform all the work necessary under the aforesaid conditions, to carry out the contract and to accept in full compensation therefore the amount of the contract as agreed to by the Contractor and the City.

The undersigned hereby declares that no reason or persons other than those named herein are interested in this proposal, which is made without any connection with any other person or persons making any proposal for the same work and is in all respects fair and without collusion or fraud; that no person acting for or employed by the City of Hartford is directly or indirectly interested therein, or in the supplies or works to which it relates, or will receive any part of the profit or any commission there from in any manner which is unethical or contrary to the best interest of said City of Hartford.

The undersigned additionally declares that they are not debarred or suspended, or otherwise excluded from, or ineligible for, participation in City of Hartford, State of Connecticut or federally funded projects (Executive Order 12549).

The undersigned certifies under penalty of false statement that the information provided in this response is true.

Submitted by ***(Signature)***		
Printed name and title	Patricia A. P. Fisher	Date April 3, 2019

(Authorized Agent of Company)

1.2 RESPONSE PRICING

Vendor to break out each proposed task and provide a summary, hourly rates and estimated hours needed for each proposed task.

(Please see response following this form.)

1.3 STATEMENT OF QUALIFICATIONS

Please complete the following information. Failure to respond to all items may result in the rejection of your response.

1. Number of years in business - 30 D-U-N-S Number: 803783315

2. Number of personnel employed Part time - 1, Full time - 16,

3. List up to six past contracts of this type/size your firm has completed within the last three (3) years:

Project	Date	Contact Person	Phone No.
.NYC Police Pension Fund - IT Security Audit	.09/2018 - Ongoing	.John Flynn, Chief Information Officer	.212-693-4460
.North Carolina Department of Public Safety - IT Security Assessment	.04/2018 - 08/2018	.Jeffery Price, Information Security Officer	.919-324-6069
.Schertz-Cibolo-Universal City Independent School District - Network Security Audit	.04/2018 - 07/2018	.Karla Burkholder, Director of Technology	.940-367-6841
.Charles Stark Draper Laboratory, Inc. - External/Internal Penetration Testing	.09/2018 - 02/2019	.Kevin Burns, Chief Information Security Officer	.617-258-2277
.Frederick County Public Schools - Technology Infrastructure External Security Pen Testing Services	.06/2017 - 06/2018	.Chris Bohner, Supervisor, Networks and Security	.301-788-3760

.PA Health Care Cost Containment Council Org. - Cyber Security Assessment	.11/2016 - 2/2017	.Rob Andersen, Chief Information Officer	.717-232-6787

4. DAS CONTRACTOR PREQUALIFICATION *(required for construction / infrastructure projects only)* DAS prequalified? □Yes □No N/A	You certify that there has been no substantial change in your financial position or corporate structure since your most recent prequalification certificate was issued or renewed, other than those changes noted in the update statement (attached).	YES □ N/A	NO □

5. ORGANIZATIONAL STRUCTURE OF BUSINESS ENTITY (select one)	□	General partnership (GP)
	□	Limited partnership (LP)
	□	Limited liability corporation (LLC)
	□	Limited liability partnership (LLP)
	☒	Corporation
	□	Individual doing business under a trade name (sole proprietor)
	□	other (specify)

6. CITY OF HARTFORD TAX STATUS / OTHER FINANCIAL OBLIGATIONS	**Hartford Businesses** – All City of Hartford taxes & financial obligations (real, motor & personal property) are current and paid in full or subject to a current and approved payment plan. Please attach RFR Affidavit.	Yes □ N/A	No □
	Non-Hartford Businesses - All City of Hartford financial obligations are current and paid in full or subject to a current and approved payment plan. Please attach RFR Affidavit.	Yes ☒ There are no taxes to be paid at this time.	No □
7. STATUS OF THE BUSINESS AND ITS CURRENT STANDING WITH THE SECRETARY OF STATE'S OFFICE	**Connecticut Businesses** - Are all required filings current with the Secretary of State and will the Secretary of State be able to issue a Certificate of Legal Existence?	Yes ☒	No □

	Out-of–State (foreign) Businesses – Have you filed a Certificate of Authority / Application of Registration with the Connecticut Secretary of State? If so, submit a copy of your filing with your response. If not, submit a copy of your Certificate of Good Standing from your state of incorporation.	Yes □ N/A	No □

8. Is your local organization an affiliate of a Parent company? If so, Indicate the principal place of business of the parent company and the name of agent for service.					
Business Name	.N/A				
Address	.				
City	.	State	.	Zip	.
Name of Agent	.				

9. List all Affiliated Businesses (attach additional sheets as necessary):

Business Name	Address	Ownership Interest %
.N/A	.	.
.	.	.
.	.	.
.	.	.

10. Based on the organizational structure of your business, provide a current listing of all corporate officers, principals, general or managing partners, limited partners, managers and members. If sole proprietorship or general partnership, attach trade name certificate filed with the town clerks office.

(Response is provided following this form.)

11. Submit copies of all required business (trade & occupational) licenses with your response.

(Response is provided following this form.)

12. Your company may be asked to submit information relative to your company's financial statements and/or a Dun & Bradstreet report may be obtained prior to receiving an award. This information will be protected to the fullest extent required by law.

13. Additional information/documentation may be requested subsequent to your responding to this solicitation.

Response to EEO Form Part V – Item 2

We are committed to hiring both minority and female workers in our highly technical field. Our president is a woman and regularly seeks out potential minority and female candidates to provide them with opportunities.

Response to Section 1.2 Response Pricing

The proposed fee for this Cyber Security project is **$181,995.00**. We anticipate that the project will take 1,103 hours at a rate of $165.00/hour. Please refer to the project plan below for details. All work will be accomplished by JANUS employees without the use of a subcontractor. Travel and expenses are billed at cost, as incurred. We anticipate travel to be minimal since the work primarily will originate from our W. Hartford and Stamford offices.

Invoicing

Invoicing for the assessment is proposed as follows:

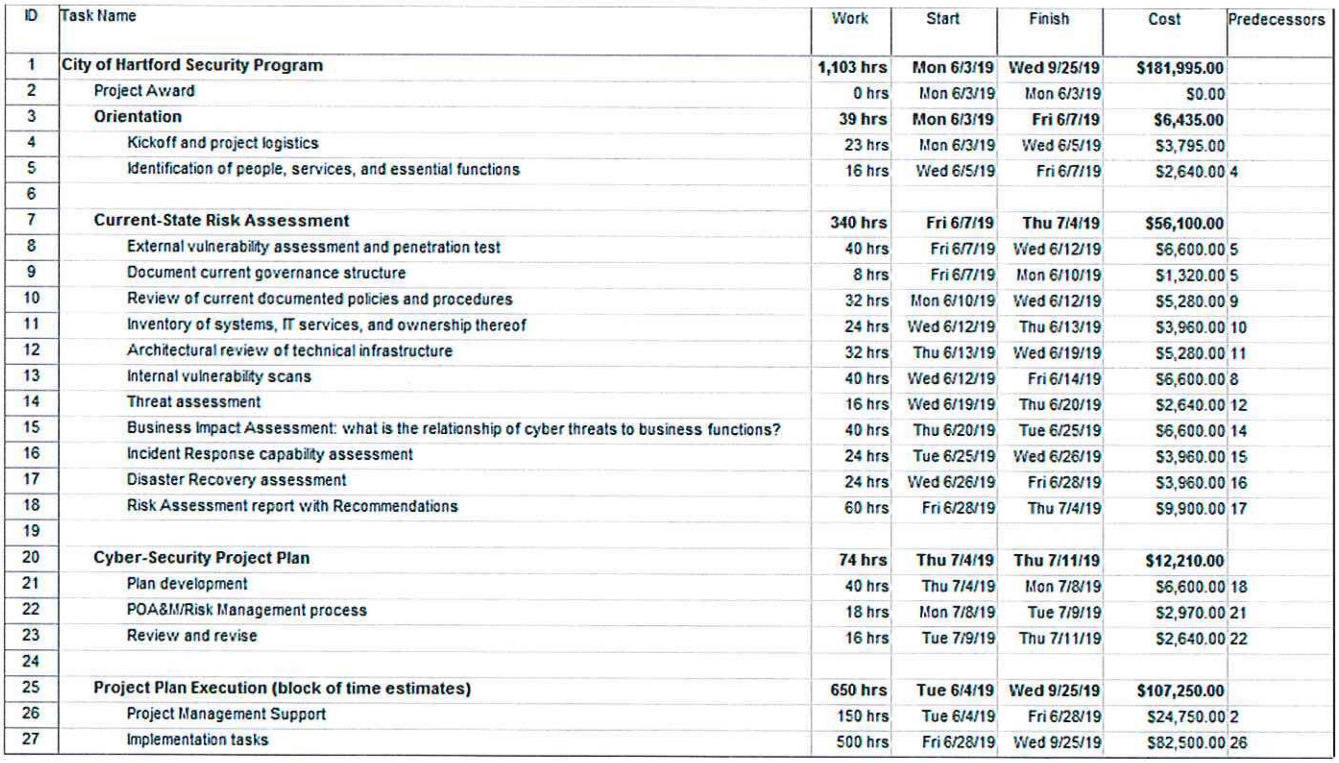
30% upon completion of the preparation period
45% upon completion of the on-site field work
20% upon submission of the draft report
5% upon submission of the final report

Payment Terms

1% discount, 10 days

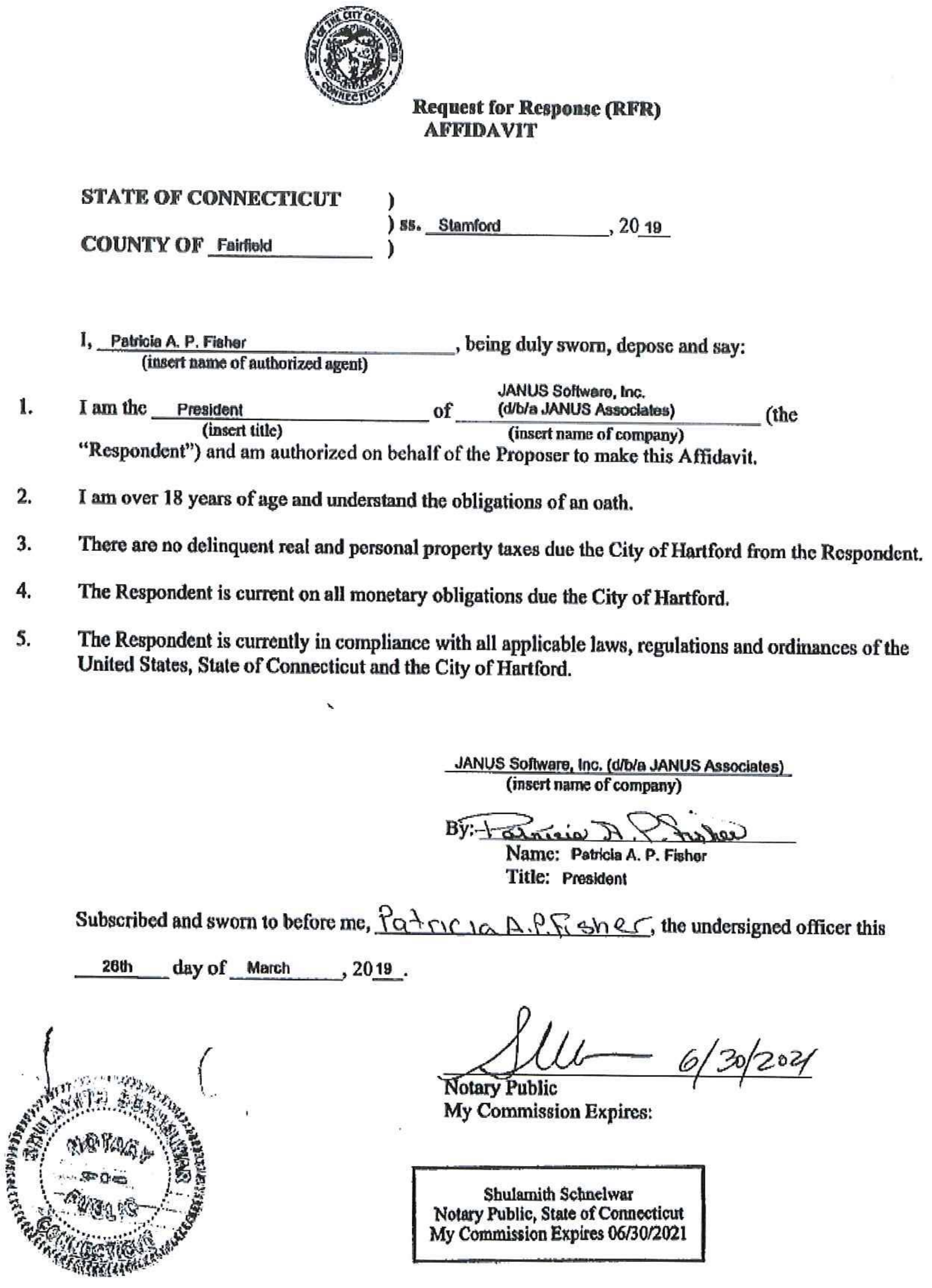
Project Plan

Below is a detailed project plan which presents a comprehensive listing of assessment tasks along with the fees for each task (and subtask).



ID	Task Name	Work	Start	Finish	Cost	Predecessors
1	**City of Hartford Security Program**	**1,103 hrs**	**Mon 6/3/19**	**Wed 9/25/19**	**$181,995.00**	
2	Project Award	0 hrs	Mon 6/3/19	Mon 6/3/19	$0.00	
3	**Orientation**	**39 hrs**	**Mon 6/3/19**	**Fri 6/7/19**	**$6,435.00**	
4	Kickoff and project logistics	23 hrs	Mon 6/3/19	Wed 6/5/19	$3,795.00	
5	Identification of people, services, and essential functions	16 hrs	Wed 6/5/19	Fri 6/7/19	$2,640.00	4
6						
7	**Current-State Risk Assessment**	**340 hrs**	**Fri 6/7/19**	**Thu 7/4/19**	**$56,100.00**	
8	External vulnerability assessment and penetration test	40 hrs	Fri 6/7/19	Wed 6/12/19	$6,600.00	5
9	Document current governance structure	8 hrs	Fri 6/7/19	Mon 6/10/19	$1,320.00	5
10	Review of current documented policies and procedures	32 hrs	Mon 6/10/19	Wed 6/12/19	$5,280.00	9
11	Inventory of systems, IT services, and ownership thereof	24 hrs	Wed 6/12/19	Thu 6/13/19	$3,960.00	10
12	Architectural review of technical infrastructure	32 hrs	Thu 6/13/19	Wed 6/19/19	$5,280.00	11
13	Internal vulnerability scans	40 hrs	Wed 6/12/19	Fri 6/14/19	$6,600.00	8
14	Threat assessment	16 hrs	Wed 6/19/19	Thu 6/20/19	$2,640.00	12
15	Business Impact Assessment: what is the relationship of cyber threats to business functions?	40 hrs	Thu 6/20/19	Tue 6/25/19	$6,600.00	14
16	Incident Response capability assessment	24 hrs	Tue 6/25/19	Wed 6/26/19	$3,960.00	15
17	Disaster Recovery assessment	24 hrs	Wed 6/26/19	Fri 6/28/19	$3,960.00	16
18	Risk Assessment report with Recommendations	60 hrs	Fri 6/28/19	Thu 7/4/19	$9,900.00	17
19						
20	**Cyber-Security Project Plan**	**74 hrs**	**Thu 7/4/19**	**Thu 7/11/19**	**$12,210.00**	
21	Plan development	40 hrs	Thu 7/4/19	Mon 7/8/19	$6,600.00	18
22	POA&M/Risk Management process	18 hrs	Mon 7/8/19	Tue 7/9/19	$2,970.00	21
23	Review and revise	16 hrs	Tue 7/9/19	Thu 7/11/19	$2,640.00	22
24						
25	**Project Plan Execution (block of time estimates)**	**650 hrs**	**Tue 6/4/19**	**Wed 9/25/19**	**$107,250.00**	
26	Project Management Support	150 hrs	Tue 6/4/19	Fri 6/28/19	$24,750.00	2
27	Implementation tasks	500 hrs	Fri 6/28/19	Wed 9/25/19	$82,500.00	26

Response to Section 1.3 Item 6



Request for Response (RFR)
AFFIDAVIT

STATE OF CONNECTICUT)
) ss. Stamford **, 20**19
COUNTY OF Fairfield **)**

I, Patricia A. P. Fisher **, being duly sworn, depose and say:**
(insert name of authorized agent)

1. **I am the** President **of** JANUS Software, Inc. (d/b/a JANUS Associates) **(the**
(insert title) **(insert name of company)**
"Respondent") and am authorized on behalf of the Proposer to make this Affidavit.

2. **I am over 18 years of age and understand the obligations of an oath.**

3. **There are no delinquent real and personal property taxes due the City of Hartford from the Respondent.**

4. **The Respondent is current on all monetary obligations due the City of Hartford.**

5. **The Respondent is currently in compliance with all applicable laws, regulations and ordinances of the United States, State of Connecticut and the City of Hartford.**

JANUS Software, Inc. (d/b/a JANUS Associates)
(insert name of company)

By: Patricia A. P. Fisher
Name: Patricia A. P. Fisher
Title: President

Subscribed and sworn to before me, Patricia A.P.Fisher**, the undersigned officer this**

26th **day of** March **, 20**19**.**

6/30/2021
Notary Public
My Commission Expires:

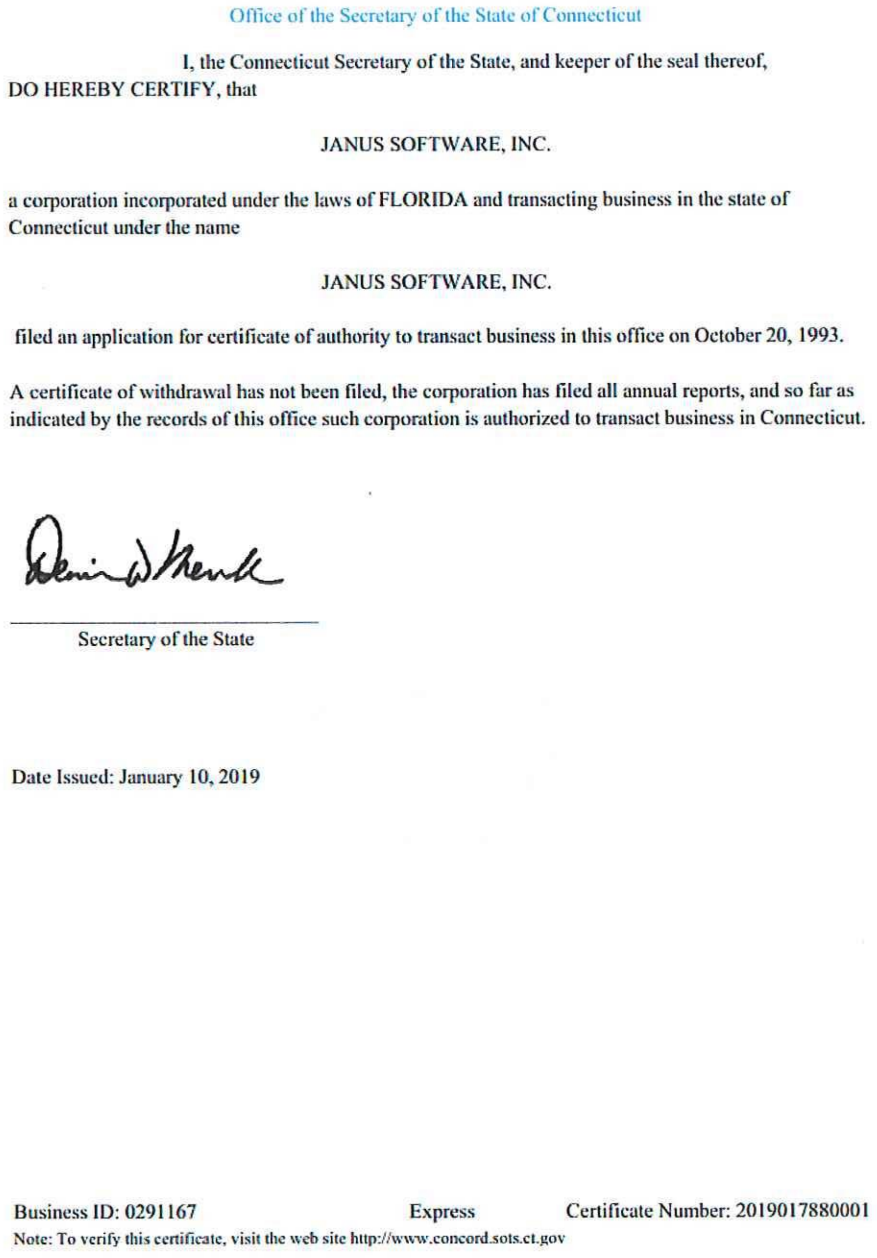
Shulamith Schneiwar
Notary Public, State of Connecticut
My Commission Expires 06/30/2021

Response to Section 1.3 Item 10

JANUS' officers include the following:

Patricia A. P. Fisher President & CEO Director	Adam G. Fisher Corporate Secretary Director
Matthew J. Lane V.P. and Chief Information Officer	Abigail Williamson Director

Response to Section 1.3 Item 11



Office of the Secretary of the State of Connecticut

I, the Connecticut Secretary of the State, and keeper of the seal thereof, DO HEREBY CERTIFY, that

JANUS SOFTWARE, INC.

a corporation incorporated under the laws of FLORIDA and transacting business in the state of Connecticut under the name

JANUS SOFTWARE, INC.

filed an application for certificate of authority to transact business in this office on October 20, 1993.

A certificate of withdrawal has not been filed, the corporation has filed all annual reports, and so far as indicated by the records of this office such corporation is authorized to transact business in Connecticut.

Secretary of the State

Date Issued: January 10, 2019

Business ID: 0291167 Express Certificate Number: 2019017880001

Note: To verify this certificate, visit the web site http://www.concord.sots.ct.gov

RFP GENERAL INFORMATION AND INTENT

2.1 General Information & Intent

2.1.1 General Information

Metro Hartford Innovation Services (MHIS) is the consolidated information service and information technology department for the City of Hartford, the Hartford Public Schools (HPS), and the Hartford Public Library (HPL) and its branches. MHIS provides a full range of IT services to its sponsoring organizations, ranging from Help Desk and PC support to telephony, data networking, user training and enterprise applications.

Securing the City of Hartford\Hartford Public Schools against cyber-attacks has become one of our highest priorities. To achieve this objective MHIS must vigorously defend against a variety of threats, both internal and external.

MHIS seeks the assistance of skilled and reputable cyber-security and organizational vendors/consultants to assess system vulnerabilities and risks, to create and assist in implementing a strategic information security program, supply Hardware & software solutions, managed security services, threat intelligence, detection monitoring, and mitigation response layers that are aligned with the City of Hartford Cyber Security initiatives.

Hartford is mid-sized city with approximately 112,000 residents, among whom are 19,000 students attending over 40 Hartford schools. As with many municipalities, Hartford is constrained by rising costs and declining revenue.

2.1.2 Intent

The City intends to identify, and enter into multiple contracts to secure the services and hardware necessary to protect the city against attack and be able to quickly recover in the event of an attack.

The City seeks the services of qualified vendors to provide Cyber Security Services. It is the City's intention to award this RFP to qualified vendors who can provide the hardware and the services requested herein. The award period will be for one year with a City option for up to three one-year extensions.

Respondents must analyze and respond to all sections of this specification and provide sufficient information and product samples (if necessary) to allow the City of Hartford Procurement Division, and MHIS to evaluate the offerings. Respondents must furnish all information as requested and complete all forms according to the section instructions. Any deviations or exceptions to these requirements must be noted. Incomplete proposals or proposals which do not comply with the requirements described herein may be eliminated from the purchase decision. The sole judge of what constitutes an acceptable proposal shall be the City of Hartford.

The City shall incur no obligation or liability whatsoever to anyone by reason of issuance of this request for proposal and specifications. The City reserves the right to reject any and all proposals for its own reasons, and to withdraw this request for proposals at any time.

2.1.3 "City" as Inclusive Label

Unless specifically indicated, all references to "the City" in this document are inclusive of all elements of the municipal government: the City of Hartford, Hartford Public Schools and Hartford Public Library.

2.1.4 Inquiries and Clarifications

The City will make every attempt to answer all questions submitted by prospective vendors. Questions and answers will be made available to all respondents via RFP Addenda to ensure consistent interpretation of the bid items.

2.1.5 Proposal Expiration

Respondents shall indicate expiration dates for pricing and include hardware model roadmaps in any proposal submitted. Expiration dates shall not be less than 60 days from the Proposal Due Date. Once a vendor's proposal has been accepted, terms and conditions (including price schedules) shall be frozen for the duration of the contract period, unless changed by mutual written agreement. Prices for labor charges (technician services) shall remain valid through the end of the contract period.

JANUS' Response to 2.1.5 Proposal Expiration

Pricing for this proposal will expire after 90 days unless an extension is agreed to by both parties.

RFP SPECIAL REQUIREMENTS

2.2 Special Requirements

2.2.1 Response Format

Respondents should return annotated copies of sections one (General Information and Intent), two (Special Requirements) and three (Scope of Services) of this document, with each paragraph noted for compliance, conditioned compliance (appropriately explained), or exceptions. All appendices should be completed in either Word document or Excel spreadsheet format (files are attached). Fields on those forms should be completed with price or requested information. Comments in those fields such as "See attached exhibit" or "See attached spreadsheet" are discouraged.

2.2.2 Supporting Documentation

Respondents are encouraged to provide any and all documents they believe are necessary to describe the service offering, and the experience and expertise of the company. We ask, however, that those documents be concise and to the point.

JANUS' Response to Item 2.2.2 Supporting Documentation

Qualifications and Experience – JANUS Overview

Founded in 1988, JANUS is America's longest operating information risk management and IT security firm. JANUS continues to serve a wide range of clients in government, healthcare, education, and industry and brings the best practices of all sectors to our projects. JANUS is a privately held, woman-owned small business (WOSB) headquartered in Stamford, CT with additional offices in West Hartford, CT; Philadelphia, PA; Baltimore, MD; Tallahassee, FL; Miami, FL; Lubbock, TX; and Washington, D.C.

Although we are certified by a variety of state and local government bodies as a woman-owned, small business we have remained in business for over 30 years due to the excellence of our offerings, our dedication to our clients, our vendor neutral results, our flexibility to meet evolving customer needs, and our ability to compete with the largest security organizations to bring needed solutions to our customers. We have focused on information security, forensics, security engineering, business resilience, and associated services as our core business since our founding and possess the depth and experience required to fulfill the City's requirements for this project and into the future.

As an independent organization that focuses on risk, information security assessment, and penetration testing, we have a natural affinity to protect our clients and bring improvements to your business processes –all designed to help you achieve excellence. We are specialists in Information Technology (IT) and risk assessment and as such, we understand that helping the City discover risks early and then making practical recommendations for mitigating them is one of the best ways we can add value to your business and protect it. We have broad experience across numerous municipal, state and federal government entities, as well as educational, utility and transportation entities, and we believe our values and skill sets will exceed the City's expectations for this project.

JANUS is not partnered with any hardware or software providers. We are not an accounting firm that augments our work with a cyber security sideline. Providing cyber security services is our core focus and specialty. The City can be assured that we have no relationships which would influence our recommendations – or accounting services to sell. This is very unusual in our business but is structured to offer you the best unbiased capabilities. As a result, we are ideally positioned to assist you with your needs. This client-centric approach has been well-honed by many similar successful projects completed each year.

A cornerstone of JANUS assessments is our explanation of business risks and problems and how what we find will affect the City's business in addition to the technical issues discovered. Every JANUS finding carries with it a delineation of the actual issue affecting business operations, providing a translation of the information and analysis into terms that are relevant to both technical and managerial personnel. This extends the value of the analysis and makes it more actionable – thus bringing greater return on investment for the City. JANUS is known throughout the cyber security industry for this unique approach.

Another hallmark of our services is quality, which is demonstrated by the professionalism of our staff, the depth and currency of our understanding of information security and network issues, and the clarity of our reports and oral communication.

A benefit of our projects is the high-quality level of the results, including our reports. We are well regarded for our reports which include sections written in plain English to help foster understanding for those who are not technically inclined. While all consulting firms position themselves as providing high quality, we have formal client feedback and independent evaluations that reinforce this concept. This translates into high return on investment for the City.

To provide a clearer understanding of JANUS' relationship with our clients and thorough deliverables, we include the following quotes from comments by our clients.

JANUS clients were asked to rate our knowledge and expertise (**10 = best; 1 = worst**):

Wyoming State Agency

Question #/Question	Rating	
2. Rate the firm's knowledge and expertise.	**RATING:**	**10**
Comments: JANUS has demonstrated its subject matter expertise each time we have engaged their services. They have also assisted with issues arising in other areas while they were on site. [Redacted] is a State agency consisting of four divisions. Within those divisions there are over one hundred programs and five direct care facilities.		

Massachusetts State Agency

Question #/Question	Rating	
9. Rate the knowledge of the vendor's assigned staff and their ability to accomplish duties as contracted.	**RATING:**	**10**
Comments: Outstanding!		

Federal Agency

Question #/Question	Rating	
9. Rate the knowledge of the vendor's assigned staff and their ability to accomplish duties as contracted.	**RATING:**	**10**
Comments: Janus has a veteran staff that saw very little turnover. Key personnel remained on the project throughout each project. Over the eleven years that I worked with Janus, key personnel left on the rare occasion due to health reasons or changes in their personal lives that required a physical move. Often they still remained on the project assisting with the completion remotely. New experienced staff was brought on board to continue Janus' quality of service. In addition, the staff has experience across all levels of information security from the mainframe, mid-tier, desk-top to all current mobile and network		

technologies. This was particularly important in an agency that employs all of the above. Janus' management style is very hands-on and regularly met to discuss the project status and make any necessary adjustments based on the technical direction of the Project Officer.

JANUS consistently receives customer comments similar to these and will ensure that our work for the City remains equally diligent and thorough.

The breadth of JANUS' technical consulting work includes virtually every business process and every information system. Our extensive knowledge of information systems includes all major technical platforms: Windows (all versions); UNIX; Linux; Novell; Apple/Macintosh; and IBM's AS/400, iSeries, and OS/390 – z/OS as well as a variety of proprietary operating systems, e.g., GE and Honeywell as well as mobile and tablet.

Having completed many projects that require vision, management, remediation, development, and IT systems analyses and assessment of large, complex organizational requirements, JANUS' consultants understand how to determine the true need, which often differs from the stated need. Our consultants blend what they hear with what they observe, factor in the challenges, and produce a clear and cost-benefit conclusion for clients. A recent statement by a Commonwealth of Massachusetts Technology Director was that every time he left the room from a JANUS meeting, he felt smarter as a result of our assistance and advice.

JANUS Capabilities

JANUS' long commitment to improving infrastructure, IT networking, application, and security, performing Independent Verification and Validation (IV&V) and risk, vulnerability, and compliance assessments as well as training has resulted in our consultants having a high-level of understanding of the issues that confront complex organizations such as those of the City. This knowledge has been essential in establishing JANUS' standing in this field. JANUS brings a rigorous focus on excellence and proven ability to provide client-centric solutions to all projects and has the business experience to understand the relative value of information and its impact on an organization. Our firm's extensive experience within a broad spectrum of settings provides clients with an objective, balanced perspective. JANUS also assists our clients in achieving a proper balance between technology needs and cost.

For our tests and assessments, we follow processes that are geared to provide you with a set of full results and recommendations that make your follow-on work easier. This is not always done by consultants, but JANUS has specialized in security, continuity, and forensics for over 30 years. We know how to relieve some of the burden from our clients by thinking through a complete project process – and we do that. In tests and assessments, we also know what you will need to do to verify our findings (if we do not) – so we take on that responsibility, thus eliminating the time and expense you would need to exert following our assessments. There are consultants who will appear to offer a less expensive solution; however, rarely will that solution be complete enough to relieve you of the many follow-on resource requirements of results verification that enable you to begin remediation. We offer a holistic solution to truly meet enterprise security needs at an excellent price point.

Service Offerings

JANUS does business throughout the U.S. focusing on information security, business continuity, regulatory compliance, and computer forensics/e-Discovery. JANUS has provided services to private industry; federal, state, and local government; not-for-profit organizations; and secondary and higher education institutions and is eminently qualified and well-positioned to satisfy the City's cyber security requirements.

JANUS confronts complex technical issues with a clear understanding and appreciation for the operational business objectives of the organization and helps align and balance operational objectives with the particular needs of our clients. We also work to enhance knowledge transfer with clients, thus enhancing the lasting impact of our involvement.

JANUS responds quickly to client needs – wherever and whenever required. Clients reap the benefit of having access to JANUS senior level people who are innovative experts, not trainees. JANUS top management is available for answers to questions and quick response. As an independent, vendor-neutral entity, JANUS is not limited by product offerings and is free to identify the best solutions to specific needs, rather than force-fitting specific vendor offerings.

Assessment Experience

JANUS has focused on security risk and vulnerability assessments within our consulting throughout our history in our quest to protect and analyze our clients' information. We have completed many hundreds. Staff has long seen the potential for major problems at clients' sites and in their systems and has striven to analyze these and/or eliminate them, depending on the project, in each of our clients' environments.

Enterprise-Wide Systems

In early 1989, JANUS took on our first major enterprise-wide engagement by conducting a comprehensive, multi-facility review and vulnerability assessment of controls for Aetna Insurance to improve incident recovery and control processes. Follow-on projects included long-term database design and implementation, application design, strategy development and business process re-engineering.

Significant business followed with firms like GTE Directories (now Verizon) in Texas and Florida, where JANUS conducted major business impact analyses advising staff how to manage risk. Additional assignments included assistance with financial record-keeping by locating, documenting, and categorizing assets to write-off outdated technology components, programs, and devices. Southern New England Telephone (now AT&T) had JANUS assess its physical and logical security capabilities, to determine weaknesses and to perform penetration testing and information security tasks.

Security Management

JANUS' breadth of experience in the security marketplace makes us the ideal candidate for security testing and management assignments. JANUS staff, through our many projects, has gained a strong understanding of the issues confronting our clients' needs and desired goals; the problems that might occur during projects; the way to structure tasks to ensure they are controllable; and the management of a variety of simultaneous subtasks. As a result, JANUS projects are completed on-time and on-budget.

Computer Forensics

With our established reputation for ethics, credentialed experts, and our vast knowledge in the field of Information Technology, it was not surprising when the legal community began to call upon JANUS to assist in the electronic discovery of evidence – a field that has since become known as computer or digital forensics.

By the end of 1998, JANUS' assignments in investigations and fraud examinations had been combined with our work on electronic discovery and breach response/prevention services to form a separate computer forensics practice. JANUS subsequently is the only firm in America to have played a prominent role in the adjudication of both the TJX and the Heartland breach cases as court-appointed experts.

E-Commerce

As Internet usage increased in both business and industry, JANUS responded to clients' e-commerce needs. Adding people to our staff who had been involved in some of the first Internet security incidents reported to the FBI, JANUS consultants were able to address increasingly complex e-commerce and Internet issues. JANUS currently provides services such as IT security strategy, manages IT implementations (as a vendor-neutral consultant), de-militarized zone design, and wireless strategy and design services, web-based consulting involving: security-conscious web design, secure web connectivity to back-office systems, virtual private network (VPN) design and implementation, biometric assessment and design, PKI enabling technologies, firewall/router/switch design implementation, and testing, illustrating a few examples. The skills gained in providing these services directly impact the capabilities to provide leading edge technical cyber solutions.

Recognizing the sophistication and forward thinking of JANUS in the Internet area, a critically sensitive branch of the federal government chose JANUS over six vendors to architect and implement secure and anonymous connectivity to the Internet in 1999. The challenge was to ensure that the entire operation could meet the organization's e-commerce needs and, at the same time, warrant that the internal data remained locked-away from hackers and unauthorized staff. The client also required flexibility to conduct research via the Internet anonymously or not, whichever suited its objectives.

JANUS' initial focus on security consulting has broadened to include all areas affecting the controlled, efficient flow and design of information.

Description of Services

We specialize in protecting clients' data and computing environments through (samples):

Security Testing & Assessment

- Application Testing
- Vulnerability & Penetration Testing
- Security Controls Assessments (SCA)
- Security Testing and Evaluation (ST&E)
- Security/Risk Assessments
- Compliance Reviews
- Social Engineering
- Wireless Assessment & Testing
- Application Code Reviews
- War Dialing
- I.C.U...MVS® Mainframe Security Auditing and Tools

Information Security Consulting & Controls

- Current-State and Future-State IT and Security Assessments
- Chief Information Security Officer Services
- Future Roadmap Development
- Governance and Risk Management
- Gap and Organizational Analyses
- Network and Security Cost Analyses
- Data Classification and Inventory
- IT and Security Design/Development & System Architecture
- IT and Security Governance
- Certification & Accreditation
- Firewall Design & Implementation
- Independent Verification and Validation (IV&V)
- Program, Policy and Procedure Development
- Metrics Development and Assessment
- Wireless Security Design
- System Hardening
- Incident Response Planning
- Convergence of Logical & Physical Security
- Implementation of Security and Controls in the SDLC
- Risk Management Program Development
- Cloud Computing and Migration Risk Assessments
- Biometrics Security
- e-Discovery and Digital Forensics
- Independent Third-Party Reviews

Business Resilience

- Business Continuity (BC)
- Disaster Recovery (DR)
- Continuity of Operations (COOP)

- Planning and Testing
- Business Impact Analysis (BIA)
- Privacy Impact Assessment (PIA)
- Data Breach Crisis Response

Education

- Secure Web Application Analysis and Training
- General Security Awareness & Training
- Curriculum & Content Design
- Computer-Based Training (CBT) Design

2.2.3 Organization

The chosen vendor must have a proven track record in the industry, and significant financial and technical in-house resources. The structure of the organization, the size and location of its sales, service, and administrative support functions are important factors that the reviewers of the proposals will consider in making an award. Respondents are requested to provide an organizational chart of the sales, service, support, and any other pertinent arms of their company. Respondents should also provide the address of their nearest sales offices, engineering office, and billing department.

Respondents are required to submit an organizational chart of the account team that will be servicing the City's account. This chart must include the names, telephone numbers and email addresses of all staff who will directly service the account and management up to the Director or Vice President Level.

JANUS' Response to Item 2.2.3 Organization

JANUS has a 30+ year proven track record in this industry for performing similar assessments and supporting information security needs for a wide variety of well-known organizations.

The type of services that the City is requesting are the type that JANUS performs every day for our clients. Current secondary education clients include the Schertz-Cibolo-Universal City Independent School District of San Antonio, Texas, Westminster School (Atlanta, Georgia), and the Charles County, Maryland School District. We also provide services for New York City. Any of these organizations could discuss our thoroughness and capabilities with you.

JANUS performs similar services for a variety of state and municipal clients as well as many others, a small sample of which follows:

A sample group of JANUS' consulting clients includes such blue-chip organizations as:

- Microsoft
- IBM

- NASA
- Charles Schwab
- Citibank

Counties and municipalities such as:

- New York City, New York
- Putnam County, New York
- Capital District Transportation Authority of Albany, New York
- Frederick County, Maryland
- Howard County, Maryland
- Charles County, Maryland
- City of Norwich, Connecticut (including its public utility)
- South Central Connecticut Regional Authority
- Westminster Schools, Atlanta, Georgia
- Charles County, Maryland
- Madison County, Illinois
- City of Naperville, Illinois
- Baltimore, Maryland – Enoch Pratt Library

Education clients such as:

- Charles County Public Schools (Maryland)
- Wor-Wic Community College (Maryland)
- College of Southern Maryland
- Sailor Network (Maryland educational and library backbone network)
- Texas State Technical College
- University of Texas
- Texas Tech University Health Sciences Center
- Schertz-Cibolo-Universal City Independent School District (Texas)
- State University of New York Buffalo
- Harford County Public Schools (Maryland)
- Community College of Baltimore County
- Anne Arundel Community College (Maryland)
- California State University at Sacramento
- Sacred Heart University
- University of Wisconsin-Madison
- University of California at Berkeley
- The McCormack Institute of the University of Massachusetts
- University of Central Arkansas

Healthcare clients such as:

- Texas Tech University Medical Center
- Texas A&M Health Center
- State of Vermont Healthcare Exchange
- State of Minnesota Healthcare Exchange
- National Government Services, Inc. (assessments of CMS healthcare applications)
- General Dynamics (assessments of CMS healthcare applications)
- RiverSpring Health
- Memorial Sloan Kettering
- Putnam/Northern Westchester Health Benefits Consortium
- Pennsylvania Health Care Cost Containment Council
- Health & Hospitals Corporation of New York
- MD Anderson Cancer Center
- The Iowa Institutes
- The Long Island Home/Brunswick Hospital

State government organizations such as:

- State of Texas
- State of North Carolina
- State of South Carolina
- State of Maryland
- Commonwealth of Massachusetts
- Commonwealth of Pennsylvania
- Commonwealth of Virginia
- State of Delaware
- State of Minnesota
- New York State
- State of Oregon
- State of Vermont
- State of Wisconsin
- Washington State
- State of Wyoming

Federal government clients such as:

- Centers for Medicare & Medicaid Services (CMS)
- Social Security Administration (SSA)
- Department of the Interior (DOI)
- Federal Trade Commission (FTC)
- Federal Reserve Board (FRB)
- National Institute of Standards and Technology (NIST)
- Federal Deposit Insurance Corporation (FDIC)
- Railroad Retirement Board (RRB)

Insurance clients such as:

- Aetna
- The Hartford
- AXA
- Travelers
- BCBS organizations in Florida, Arkansas, New York, Pennsylvania, Washington/Alaska, South Carolina

Healthcare clients such as:

- Memorial Sloan Kettering
- Health & Hospitals Corporation of New York
- Texas A&M Health Center
- MD Anderson Cancer Center
- The Iowa Institutes
- The Long Island Home/Brunswick Hospital
- Department of Health & Human Services (S. Carolina)

Utilities such as:

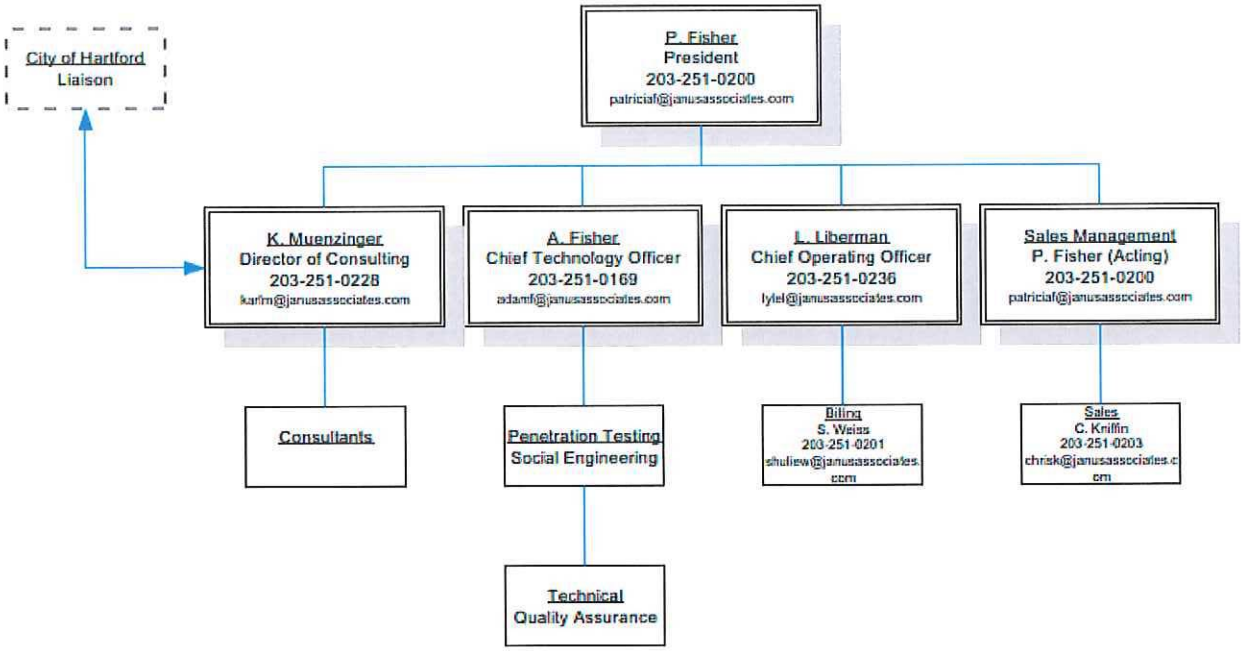
- Santee Cooper Power Company of South Carolina
- Occidental Petroleum – Permian Basin of Texas/New Mexico
- Pacific Gas and Electric
- New York Power Authority
- Massachusetts Water Resources Authority
- Norwich (Connecticut) Public Utility

Not-for-profits such as:

- The Brookings Institution
- Amnesty International
- Save the Children
- The Pine Street Inn of Boston (the largest homeless shelter system in the U.S.)

JANUS' Stamford Connecticut office will lead this project and service your account. Our West Hartford location will provide lead technical services. Other JANUS locations include Philadelphia, Pennsylvania; Baltimore, Maryland; Washington, D.C.; Tallahassee, Florida; Miami, Florida; and Lubbock, Texas.

JANUS Organization Chart



2.2.4 References

Respondents are required to submit a list of three clients, similar in size and service requirements to the City. Please also provide a contact name of the primary contact with each client, who may be contacted to provide reference information.

JANUS' Response to Item 2.2.4 References

Karla Burkholder, Ed.D.
Director of Technology
Schertz-Cibolo-Universal City ISD
1060 Elbel Road
Schertz, TX 78154
Phone: 940-367-6841
Email: kburkholder@scuc.txed.net

Richard Fantozzi, Jr.
Software Architect

Capital District Transportation Authority
110 Watervliet Avenue
Albany, NY 12206
Phone: 518-437-8322
Cell: 518-221-8137
Email: richf@cdta.org

Kevin J. Burns
Chief Information Security Officer
Draper Laboratory
Information Technology Division
555 Technology Square
Cambridge, MA 02139
Phone: 617-258-2277
Cell: 617-997-2771
Email: kburns@draper.com

2.2.5 Certifications and Manufacturer Affiliations

The City requires that the successful respondent and partners be CJIS compliant and certified by the original equipment manufacturer to sell, install, maintain and repair the equipment and software in its proposal and or provide proof of partnerships and certifications supplied in your response.

JANUS' Response to Item 2.2.5 Certification and Manufacturer Affiliations

JANUS is CJIS compliant. JANUS is a Cyber Security and Privacy Consultancy therefore we do not sell hardware/software solutions.

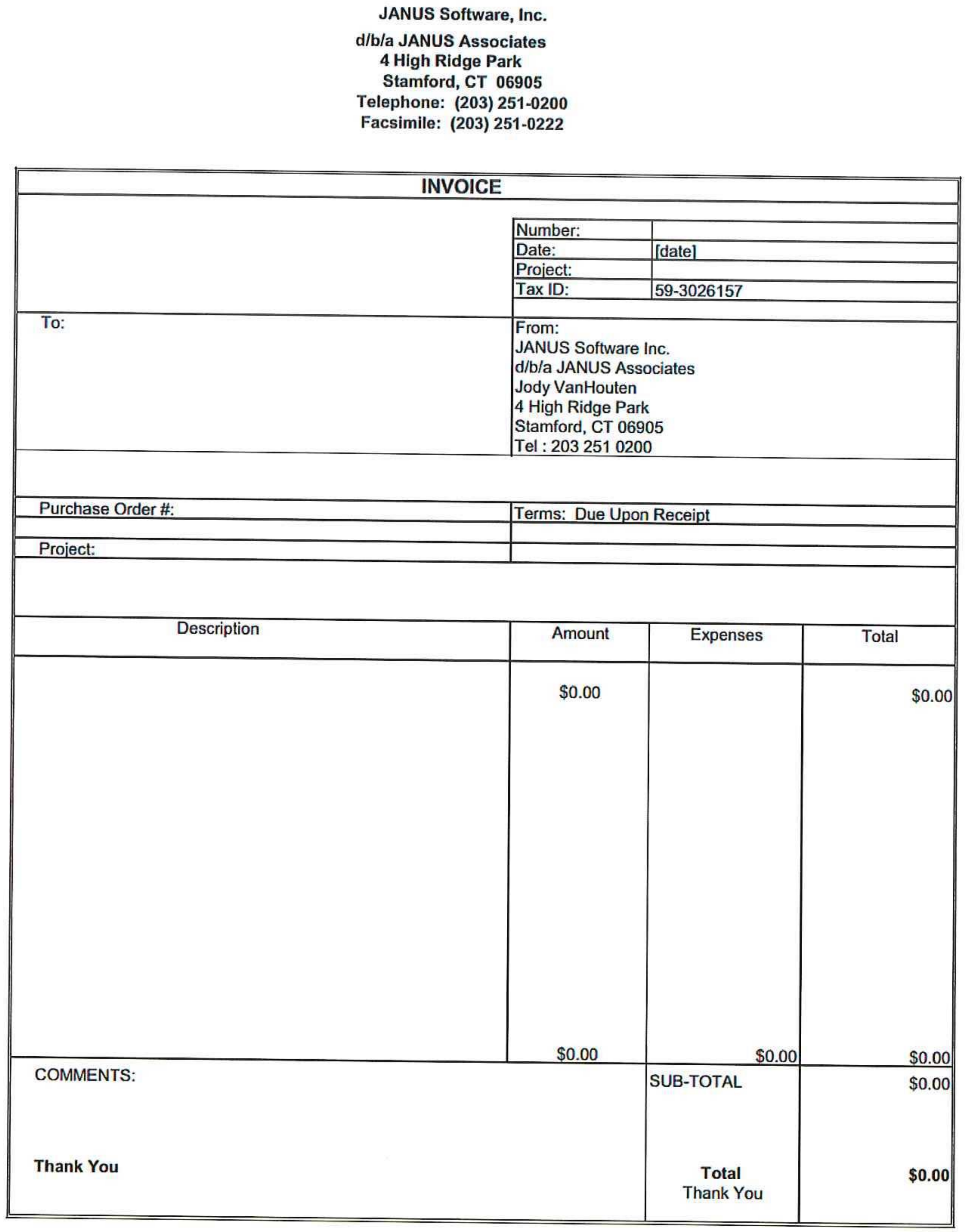
2.2.6 Sample Documents Required

Clear and proper record-keeping is fundamental to the goals of open and transparent government, and E-Rate program compliance and success. To that end, we require that respondents provide a sample packing list, invoice, asset delivery and statement on account reports. Hartford requires a monthly statement on account for our Finance Department and a quarterly asset delivery report. See Exhibit A & B for samples.

JANUS' Response to Item 2.2.6 Sample Documents

JANUS is submitting on the following pages a sample Invoice and a sample Transmittal Letter which accompanies deliverables. That is the only form of asset delivery utilized. We will customize the type of asset delivery statement the City requires; however, with services there are rarely any assets delivered. JANUS does not utilize packing lists.

Sample Invoice



JANUS Software, Inc.
d/b/a JANUS Associates
4 High Ridge Park
Stamford, CT 06905
Telephone: (203) 251-0200
Facsimile: (203) 251-0222

INVOICE

Number:	
Date:	[date]
Project:	
Tax ID:	59-3026157

To:	From: JANUS Software Inc. d/b/a JANUS Associates Jody VanHouten 4 High Ridge Park Stamford, CT 06905 Tel : 203 251 0200
Purchase Order #:	Terms: Due Upon Receipt
Project:	

Description	Amount	Expenses	Total
	$0.00		$0.00
	$0.00	$0.00	$0.00

COMMENTS:	SUB-TOTAL	$0.00
Thank You	**Total** Thank You	**$0.00**

Sample Transmittal Letter

JANUS
ASSOCIATES

[Date]

[Addressee]

Dear __________:

This letter confirms delivery of [what is being delivered] completed on [date]. This deliverable consists of:

- [Itemized list of what is being delivered.]

We thank you for the opportunity to work with [name of organization]. We look forward to further successful collaboration with you in the future.

Sincerely,

[Name]
[Title]

Acknowledged by:

____
[Customer Name]
[Customer Title]
[Date]

JANUS Associates Phone: 203.251.0200 **4 High Ridge Park** www.janusassociates.com **Stamford, CT 06905** Fax: 203.251.0222

2.2.7 Caution to Respondents

Failure to meet or fulfill the above requirements in full may disqualify your response.

RFP Scope of Services

2.3 Scope of Required Services

The Scope of Work that follows is to be used as a general guide and is not intended to be a complete list of all work necessary to efficiently develop and execute a security program for the City of Hartford\Hartford Public Schools.

The Scope of Work will generally require the tasks identified below. The Strategic Information Security Program ("Cyber-Security Program") is conceptually divided into the following components:

Objectives of the Cyber Security Program

MHIS requests the assistance of skilled cyber-security and organizational firms to evaluate the City's current cyber security risks, create and implement a strategic information security program. This Cyber-Security Program is expected to be built upon well respected cyber-security frameworks, methodologies, and standards, such as, but not limited to:

- Microsoft Operations Framework ("MOF")
- National Institute of Standards and Technology ("NIST")
- Health Insurance Portability and Accountability ("HIPAA")
- Payment Card Industry ("PCI")
- Family Educational Rights and Privacy ("FERPA")
- Department of Homeland Security ("DHS") Security Evaluation Tool ("CSET"), and
- Cyber Security Evaluation Program ("CSEP") Cyber Resilience Review ("CRR")

The successful proposer will be required to select the frameworks and standards best suited to the cyber-security and organizational needs of the City of Hartford. At a minimum, the Strategic Information Security Program ("Cyber-Security Program") must:

a. Identify and track technology-related risks across the City and Schools; allowing these systems to be managed to acceptable levels of risk.

b. Implement an acceptable governance framework and associated operating principles that are able to identify, assess and mitigate cyber-risk, including cyber-attacks that jeopardize operations and security.

c. Develop and implement assurance and audit related activities.

d. Assess Cyber-Security Vulnerabilities and Risks by performing an independent external scan and vulnerability assessment (penetration testing) at the beginning of the engagement.

e. Evaluate existing policies, practices, procedures, guidelines, procurement mechanisms and risk reporting structures; assess their effectiveness in managing information technology risk throughout the City and develop a five-year information security plan aligned to the City of Hartford goals and objectives. The Assessment must review current organizational structure and the availability of internal resources in support of the five-year information security plan.

f. Evaluate existing governance and provide recommendations to the City of Hartford, through which MHIS can effectively prioritize internal resources in support of the Cyber-Security Program and ensure material risks to stakeholders' interests are identified and addressed in a timely manner.

g. Review existing MHIS architecture and operational practices across the City and Schools, assess MHIS ability to identify exploitable vulnerabilities, and gauge MHIS ability to respond to cyber-attacks in accordance with digital forensic and incident response guidelines established by US-CERT and the U.S. Department of Justice.

h. Complete a section-by-section effort to identify and track risk associated with the adoption ownership and operation of all systems owned by or operated on behalf of the City\Schools, and prioritize these risks in accordance with their potential impact to the City's business objectives.

i. Develop a systemic and structured approach to identify and track technology-related risk across all City\School systems that may adversely affect their ability to meet its business goals and objectives.

j. Identify systems and associated infrastructure representing the highest potential risk and perform a cyber-security assessment of these high-risk.

k. Assess if current data backup and recovery policies allow the City of Hartford to recover from a major breech. Assist with the creation of an incident response plan.

Sample Penetration Testing Methodology and Approach

You have requested assistance of cyber-security firms to evaluate the City's current cyber security risks, and to create and implement a strategic information security program. That is exactly what JANUS does for our clients. We regularly work in all the frameworks, methodologies, and standards you have identified, including others.

First, we will meet with City stakeholders to select the most relevant standard for your operations. Among other standards, it will most likely need FERPA, PCI, HIPAA, and NIST focus. It also could likely require IRS 1075 standards for City taxes, if you need to conduct any reporting or receipt of information to/from the IRS.

Most organizations are beginning to move toward the federal Risk Management Framework as a consolidation occurs within standards. This would assist the City in compliance if it ever receives federal grants. JANUS can guide you towards this, as well as work to implement it, establish metrics to manage the successes of the program, and monitor compliance with it.

We can guide assurance tasks and help you develop plans, processes, procedures that our clients regularly need to comply with your selected standards and assist with audit-related activities that are designed to focus on cyber issues.

We also regularly develop strategic plans and provide Plans of Action & Milestones (POA&Ms) and roadmaps to guide progress on the strategy, all geared toward your 5-year plan. You have requested this to be an assessment and we have many clients who can attest to our policy/procurement/plan assessments and the value they bring to helping you determine what you need to embark upon to achieve your goals. Because our staff has so many years of experience they have significant expertise in assessing organization structure. Our internal resources can provide expert cyber skills in any of the tasks that you might have. Part of the assessment should be your governance structure and how the cyber security program is managed and measured. We regularly perform these types of tasks for our clients and our Connecticut staff will lead this effort.

Our technical staff in Connecticut will also help you evaluate your architecture and operational practices for the City as well as the schools and the IT department. JANUS regularly provides these services to our clients.

In identifying and tracking risks of the City/Schools, in subsections h - i we are assuming you are focusing on data classification to determine sensitivity and operation of systems. Many institutions are currently focusing on this type of task to better understand where significant risks reside and what resources should be applied to better managing risks. We are finding that our elementary and secondary school clients are particularly focused on this but their attention to insider threat is also growing rapidly. We can address both of these with you.

Our reports are clear and concise. We provide executive summaries that are graphical and that provide a quick overview graphically of what executives need to be concerned with and we also present highly detailed findings and recommendations that will lead technical people to correct conclusions about remediation steps that will be needed.

Assessing data backup and recovery policies is a regular task of JANUS consultants. However, it is not simply the policies that are critical for today's needs. How the policies are interpreted and implemented has become critical, particularly with the advent of ransomware; namely, it does no good to have a thorough policy if the backup remains connected to the network because ransomware attackers are now able to move throughout the network and attack all backups except those off-line. JANUS understands all the elements of backup and recovery policies and needs and will assist the City with them.

Scope of Services

JANUS' Approach and Methodology

Projects such as this are a specialty of JANUS'. From our over 30 years of experience and having worked with a large number of organizations, we understand the significant issues that large, complex organizations must manage – particularly the need to protect City employees and constituents and have the security infrastructure to do so. While certain controls must be met, particularly those dealing with regulations (federal/state/city security policies, regulatory requirements, etc.), we regularly need to work with our clients to find creative ways to accomplish this without recommending the expenditure of excessive amounts – often through compensating controls. We understand these types of projects and, although we have developed thorough methodologies that have been honed from many hundreds of similar tasks over our history, we understand how to work with our clients to ensure security but also usability in your particular environment. We have a strong, yet flexible methodology but we also offer flexibility in meeting your needs. Since we are vendor neutral and sell no products or software, we will provide an independent perspective and support you with no conflicts of interest that might result from any other involvement with the City.

No matter what type of security assessment, strategy, or plan is being designed, undertaken, or implemented, today's approach must be based on best practices but also be flexible to meet business needs. This means your organization's priorities must first be understood, and then your security components must reflect these business realities. Not all vulnerabilities create the same level of risk for an organization, and not every organization has the budget or personnel to mitigate every risk. A second important component of this methodology is a risk acceptance component, i.e., determining which risks the City might be willing to live with, and which you are not.

Although this sounds quite simple and straightforward, it is not. Frequently, we review assessments and tests, in particular, completed by other vendors and find them lacking in both thoroughness and quality. For example, many firms utilize Nessus for parts of their security assessments as well as penetration tests but specialists such as JANUS understand that Nessus only examines certain ranges – many are left out. Some regularly used Nessus plug-ins also provide misleading information for which our staff understands how to compensate. For reasons such as these it is critical to use combinations of tools in addition to our manual testing, which we do to ensure a comprehensive result.

Differentiator

Ability of JANUS staff to:

1) Understand the weaknesses of commonly-used tools such as Nessus and compensate; and

2) Have such significant experience with tools such as Nessus that we understand its weaknesses and know when not to accept a Nessus result because it is erroneous.

Value to Our Client

Results are accurate and fully investigated.

Our clients inform us that they are regularly presented with the results of automated scans or appliance-based outputs that no human has analyzed and after which they are left to determine what next to do to find the actual problem that caused the finding. Often, rather than identifying a risk, these simply identify a symptom of the risk. This is much simpler than finding the crux of the underlying problem and results in clients being forced to undertake significant additional work after the vendor has left. We do not do this. As one client recently put it – we use a "hands on" approach. In other words, we verify each finding to determine if it is a false positive or is a real issue for the City. This structure holds for all of our assessment types.

Differentiator

"Hands-on" analysis of automated results to ensure accuracy and thoroughness. Manual manipulation is a part of the JANUS methodology.

Value to Our Client

Ability to immediately understand the source of the problem, not simply the most obvious symptom, and what is needed to remediate potential exposures.

We also find that other firms follow a prescribed scanning process with little capability to be flexible to meet an organization's unique environment. Although we have a well-tested process, we also are intensively tuned in to your specific needs. Our clients very often provide us with feedback on previous projects and tell us that we are a very different type of company – one devoted to searching out critical vulnerabilities and helping our clients understand them and how to mitigate them. We have performed similar projects for many years and our consultants have a clear understanding of the difference between a risk and a symptom. The result is that our remedies are appropriate to the solution of underlying problems, and do not simply mask visible concerns.

Differentiator

Flexibility. Our combination tool/human-oriented methodology allows us to determine when a different approach might be needed to illustrate a specific problem. Also, we are tuned into your overall project needs so that, if a change in direction is needed (within the hours allocated for the project) we are happy to work with you to achieve your goals.

Value to Our Client

Meets your project goals even when changes have occurred between completion of the solicitation and the everyday operations of the enterprise.

Because security assessments, penetration tests, and governance projects are all core specialties of JANUS, our broad experience and deep expertise allows us to complete more focused analysis at a greater depth than most other security organizations. The result is that the City will receive greater value for your expenditure. This, in turn, will allow you to structure a stronger program, and bring additional value to your operation over the long run.

Blended Methodology

In completing the initial tasks of this project, testing and assessing, many organizations make the mistake of utilizing an IT person – who has programmed on a specific operating system or network and is therefore assumed to understand security, to conduct the assessment – even though most sites incorporate a variety of platforms or environments. Rarely are other companies, who are usually primarily IT or accounting organizations – not security specialists, cross-trained in the specific security and threat elements of multiple operating systems, application assessments, and how to move through the security of many different types of networks (e.g., Ethernet, Token Ring) and platforms (Windows, UNIX, Novell, proprietary, and IBM MVS). By making assignments this way, many vulnerabilities are not found because the consultants rarely possess in-depth knowledge of all the security elements that are needed. They only recognize potential problems that fall within their realm of experience. As security specialists, not simply IT people, our staff is able to cover *all* environments, not only the ones most often seen.

Our security assessment experience crosses many industries, environments, and types of organizations. Consistently, this experience indicates that some of the *most lethal* vulnerabilities and risks come from network/operating systems combinations or where the boundary of applications meet operating support systems. Moreover, such combinations are more likely to be known by those with some knowledge of the systems (such as a disgruntled employee, casual vendor, or hacker) which makes them even more potentially dangerous. In addition, business partners are opening up far greater risks to organizations so how they integrate their work into City systems and processes is critical to understand. We assign people to our projects who are both experienced security process/network/ application engineers and platform specialists. As attested to by our references, this "blended methodology" has been effectively employed and polished through many projects. This methodology also results in cross-trained engineers who will bring a high-level of varied experience to the City's project.

Team Effort and Knowledge Transfer

We consider each engagement a team effort; i.e., an effort shared by us and our client. We will work diligently to ensure that we impart as much knowledge to City staff as we can during the project period so that the on-going value of the project is even greater than anticipated. This has been a highly successful strategy for our clients in the past. We believe knowledge transfer is an important component of our work.

Differentiator

Knowledge transfer – JANUS staff welcomes client personnel to work with us or ask questions about why we do what we do.

Value to Our Client

Your staff will receive additional knowledge about the security of your systems and applications.

Our staff members are required to operate within a very well-controlled structure for the work. We all understand that, as professionals, we must not undertake any activity that might harm a client or reflect badly on our organization. To begin these types of projects, assigned staff may not start activities until we have been provided a Letter of Authorization* from you authorizing access to information. Once we have received this letter, the assessment begins on the basis of the agreed-to scope.

A lead is appointed for each project and monitors all activity to ensure that tests are appropriate and thorough. Periodic status meetings are held with your representatives and high-risk problems, if found, are immediately brought to your attention. While our security and network assessments do include known weaknesses and vulnerabilities and so utilize automated tools, our consultants also seek to go far beyond this by looking at complex interactions between diverse applications and other network components. Hacker methodologies are considered when appropriate and applications are examined carefully to determine the likelihood of exploitation.

Technical Currency and Results

Our staff is experienced and technologically current since we are constantly performing tasks similar to those requested by this project for a wide variety of public and private sector clients. In addition, our Chief Technical Officer is in charge of providing current and improved tools for the technical staff. He investigates possible additions to our toolbox and when he decides that one fits our needs, he prepares it and provides "learning lunches" for the staff to better understand it and how to use it. He also maintains a server infrastructure that is a practice platform where new tools are utilized by the staff to thoroughly practice with each. He changes out the potential vulnerabilities of the practice environment regularly so that the skills of the technical testers must be continually challenged.

Our technical staff spends considerable time researching new exploits and solutions. An example of this is the "WannaCry" ransomware exploit of May 2017. After the first rush of exploits over the weekend of

* We will provide a suggested format.

May 12 - 14, the next "weaponized" iteration became known on May 16. On the morning of May 16 JANUS technical staff already had this exploit in our research system and were exploring it to determine what recommendations could be provided to withstand it. We focus on staying up-to-day, such as this, for all our clients.

In our projects for clients, results are always investigated, where allowed, to ensure that "false positives" are not left with a client and to ensure that our recommendations relate to the actual problem, not simply a symptom of the problem. This is a major differentiator between us and other firms. We have seen, as an example, firms reporting that a client needs to enforce its security policy. However, this is not a good-enough finding for you to be able to remediate. We work at a deeper level to determine why the policy is a problem:

- Does the client lack a policy that staff needs to follow?
- Is the policy weak and therefore, staff members are not carefully directed in what to do?
- Is the staff simply not following the prescribed policy?

Each of these three possibilities requires a different remediation/mitigation solution. With many firms, the client would need to deduce what the correct remediation might be; we tell you – thus saving you the time and skill needed to determine a potential solution yourselves – or, even worse, to remediate incorrectly based on only partial information.

Differentiator

JANUS finds the problem, not simply the symptom.

1) As security experts we understand the difference; and

2) Understand when the tools have not portrayed the actual problem correctly.

Value to Our Client

1) Find your actual problems so you remediate correctly rather than for something that does not actually create an issue; and

2) Greater value for your expenditure.

Non-Destructive Analysis

We operate in a non-destructive manner. We do not break into systems, unless specifically directed to and where we are in close contact or being monitored by client representatives. We will simulate possible avenues of attack (particularly when assessing applications and network components or desktops) but will not unilaterally carry out exploitation unless you request it. We may discuss the need to illustrate a problem and your staff will determine to what level we should go. This is our standard mode of operation.

Testing

We conduct testing that determines if your program is being implemented effectively and if you have controls in place within the parameters of rules-of-engagement that are specified pre-engagement by you (e.g., no penetration or no exploitation of vulnerabilities). We are professionals and, as such, adhere to business-like methods for our assessment projects. Typically, that translates into "no surprises." Our team will work to assess thoroughly and diligently, while ensuring the continuity and safety of your operations.

For the more technical areas of an assessment, utilizing a sampling methodology, JANUS staff uses the means appropriate for the type of network, application, and infrastructure components found accessible. Further, we assign security engineers knowledgeable in those systems, not simply employees who can run a scanning tool. This is very important since interpreting scan results is a major element of all testing projects. Manual interpretation must be done by experienced, highly trained personnel, such as we provide, or major problems will be missed. While this affects cost, it provides lower total costs later on to the City – who would need to do this prior to remediation if we did not do so.

Having a deep understanding of security is needed. Simply assigning auditors who work from checklists to determine compliance with requirements or to present you with automated tool output is not a thorough project. While doing so will lower initial security assessment costs somewhat, it provides much higher total costs to the City – because your staff will need to do significant additional interpretation prior to remediation to know exactly what remediation to apply. We do this work for you, thus lowering your overall security spending.

Differentiator

Expert knowledge – tool results can be misleading. Experts such as JANUS must interpret results from multiple tools to ensure that findings are accurate.

Value to Our Client

1) Pinpointing the cause of the problem; and
2) Saving our client extensive time in which it would need to conduct additional investigation and interpretation before any remediation could begin.

The other half of the equation is the analysis required by a project such as this. This necessitates actually understanding the complexities of what security issues or vulnerabilities might exist across the entire City and testing specifically for those as well as possible misconfigurations, new variants, and problems with how boxes are inter-connected to result in problems. This is becoming more complex each year and our people study constantly to remain ahead of changing needs.

We offer detailed reports of findings that go beyond merely stating what the security issue or vulnerability is. Our reports include the particular impact each will have on your organization along with specific recommendations for remediation or closure.

When possible, JANUS prefers to work from a detailed test plan which we prepare prior to beginning the testing. In this way, thorough testing can be conducted without gaps or overlap. This core test plan is helpful to JANUS consultants in structuring their time and for our clients in understanding what is being examined, and when.

Manual Verification

Manual verification is an essential component of all assessments, to determine the actual risk that a reported vulnerability may pose in the real world. Automated scans identify network behaviors that are consistent with known vulnerabilities, but these scans will frequently misidentify vulnerabilities, producing "false positives." Automated scans also produce lengthy reports filled with technical jargon and theoretical risks which may not correspond to actual business impacts.

Potential vulnerabilities must be inspected using manual methods to verify that the vulnerability is real. After each vulnerability has been verified, it must be further tested to prove that it can actually be exploited during an attack. Manual verification provides the practical insight needed to prioritize risks and to help the City form your action plans for remediation.

We outline, in the following sections, how we anticipate structuring the initial portions of this project and implementing the steps of the tasks so that we follow a logical progression, from the outside, to inside.

1 *Preliminary Activities*

As soon as possible after the project award has been communicated, a pre-kickoff teleconference is scheduled. In this phase, we launch the project management methodologies and communication protocols by which subsequent phases are governed. This phase typically begins with a conference call with the primary contacts for the project and discussion of the specifics of the project. Agenda topics may include the following:

Pre-Kickoff

Pre-kickoff agenda topics may include the following:

- Confirmation of scope and deliverables;
- Overview of our process, including a high-level project schedule;
- Roles and responsibilities of key participants;
- Agree upon procedures for project related communication and sharing of confidential records;
- Initial document request list;

- Arrange for letters authorizing testing (to be carried by JANUS consultants at all times during the testing); and
- Schedule for the full project kickoff meeting (prior to internal testing).

Our understanding of scope, communication methods, roles and responsibilities, schedules, and other project management topics will be collected into a plan which will guide our testing, allowing us to move promptly through the tasks (to make it efficient for your staff) and utilizing multiple staff who will, by virtue of the structure of the plan, obtain equally high quality results. Additional components that are included in the kickoff teleconference include the following:

- Review terms of the project;
- Arrange for necessary access permissions;
- Arrange for letters authorizing testing (to be carried by our consultants during the testing);
- Review the work plan to finalize the timing of off-site and on-site work;
- Agree upon reporting and communications methods;
- Finalize rules-of-engagement;
- Discuss anticipated impact (if any) of the testing;
- Identify technical and other documents required by us;
- Introduce City and our project staff and review roles;
- Exchange contact information;
- Discuss automated tools to be used in the engagement; and
- Other logistics.

In addition, because we work from a documented plan designed to offer consistency/thoroughness, we will produce this during the earliest phase of the project. This will be discussed with the City to ensure its focus and accuracy.

Kickoff Meeting

We will conduct the project kickoff meeting at an appropriate point in the project and at a time to be mutually agreed upon between us. During the kickoff, we will request a short introductory session delivered by the most appropriate City staff members about the City security environment that will be tested, the status of the existing risk management program and strategy overall, network architecture, etc. (this will take place after the external vulnerability scan/penetration test). This provides JANUS engineers with a basic overview of your methods and operation. JANUS also requests a presentation on organizational structure, overall network components, and the network security elements in place. Also beneficial is information about your security objectives as they relate to your risk tolerance/risk aversion profile, anticipated growth/needs, etc.

In addition, we will refresh everyone on the pre-kickoff items we decided upon together that formed the general foundation upon which we built our plans so that both the City and JANUS have a common understanding of where we are beginning, how we plan to undertake the work, and the needed logistics and communications mechanisms.

Post-kickoff Activities

In our experience from similar projects, the kickoff is a time when the project team starts focusing on specific details of the engagement. While the kickoff meeting is not always the time to get too far into the details, the following topics need to be addressed during or shortly after the kickoff.

- Clarification on roles and responsibilities in the City's project, with the understanding that specific designated individuals will be interviewed during the assessment process.
- Are there any electronic security controls that are not applicable or are out of scope?
- What documents are being requested, and what supporting documentation exists?
- Which specific systems or interfaces will be subject to technical review?

Any open questions are typically addressed within three days of the kickoff meeting. At that point we will finalize our plan and be deep into preparation.

Communications Plan

After the pre-kickoff conference call, two tasks are addressed: secure communications, and our testing plan. Establishing a trusted protocol of sharing confidential information is a top priority to address at the earliest stages of the project. If the City has a preferred solution for sharing confidential documents, we will adopt the City's methodology. We also offer, at no charge, to provide a secure web portal dedicated to the assessment. This web portal utilizes encrypted communication and strict access controls for trusted sharing of files. In addition, we will use encrypted Zip files when sharing documents with participants who do not have access to the portal. We will never include unencrypted confidential information in email. The specific methodology(s) chosen should be determined prior to the beginning the project in full, so that the agreed upon communication procedures can be described to all project participants at the kickoff.

We also recommend that regularly scheduled status meetings be held after the kickoff and throughout the life of the project.

External Assessment – Penetration Test & Vulnerability Assessment

At a time to be mutually agreed upon as soon after kickoff as possible we will conduct focused external security testing of the public network infrastructure to identify ports and services enabled which might allow us to reach selected applications, servers, or other areas of the City environment. In this testing, JANUS consultants seek to gain as much knowledge as they can about the City's Internet presence and web-focused applications using resources available to any technical person via the Internet.

First, we will attempt to gain access to the network outside the perimeter by penetrating, or circumventing, protection mechanisms in a non-destructive manner without being provided any information by the City. To accomplish this, JANUS anticipates that the testing will encompass at least the following:

- Evaluation of IP address range
- Internet vulnerability scanning
- Lateral motion within the network
- Internet firewalls
- Web/Email server(s)
- Other devices identified during testing

It should be noted that our consultants might veer from the test plan to explore unexpected routes into the network that may surface during the testing. From this testing, we will determine where exploitation can occur and begin to document those possibilities.

Approach

This testing will involve what we label our "**Eyes-Shut**" testing. This means that JANUS performs an examination, beginning with scanning, from outside, through the Internet with no City-originated User IDs or information; rather, we will operate initially utilizing only the predetermined IP ranges provided by the City to avoid disturbing other organizations. The "**Eyes-Shut**" approach is described below. Potential target hosts are identified and screen prints (as well as any other pertinent documentation) are taken during the testing to document vulnerabilities found.

"No Knowledge" or "Eyes-Shut" Testing

In this scenario, we typically receive no information regarding available information, User IDs, passwords, remote access numbers, etc. except the IP address range, if agreeable (to avoid accessing other organizations' data). Initial port scans and Internet research with appropriate tools determine what can be seen, what services are running, what remote and live hosts we can identify (and/or reach), and what can be accessed, thus providing initial information on vulnerabilities that may exist.

We focus on Internet-facing security devices, seek to discover the presence of open ports and unneeded services, evaluate the devices and systems for possible configuration errors/weak security settings, review the public network security architecture and remote access for potential weaknesses, and assess the resiliency to malware and malicious code. This will also examine how network vulnerabilities might be exploited, as well as what we can access as unauthorized persons.

While "**Eyes-Shut**" testing could go on for weeks (i.e., a real hacker who wanted to penetrate the environment could spend as long as it would take to gather the information needed), from a cost/benefit standpoint, we believe a limited engagement is more appropriate. A limited engagement will still provide a realistic hacker's eye view of systems. It will *not* yield information about the obscure pathways into the systems, nor will it simulate the view that might be gained by those who already have some information (such as a disgruntled employee). It will, however, reveal most issues.

We will also request you to be cognizant of what activity your incident response team observes. If you wish, we will "step up" the level of activity – from stealthy to more obvious – to try to determine at what level our activities are observed, and we will report this information in our deliverables. To prevent being blocked from testing, we will work with those City staff members whom you designate.

At the end of this cycle, activities and findings are documented, results analyzed to determine the level of risk, and appropriate mitigation strategies developed. These are then integrated into the project assessment report.

Where possible, we will also seek to address the following (among other items), if they are able to be determined as posing as an external tester:

- Implementation flaws/code bugs that could open a vector to attack downstream application software;
- User authentication security;
- Access control mechanisms;
- Data communications integrity and confidentiality protections;
- Session management protections against attacks such as man-in-the-middle, session hijacking or session replay;
- Cryptographic module integrity;
- Adequate input validation protections against attack; and
- Presence of adequate auditing/logging of system events to preserve non-repudiation integrity and assess the capabilities present to detect/alert on targeted attacks or malicious activities.

"Eyes-Open" Review - Optional

After the major share of the "**Eyes-Shut**" portion of the assignment is complete, typically, a second phase of the external assessment begins, if you wish. In this, we shift from uncredentialed to perform some tests as a low-level user such as a vendor – but from outside your network. Although this is optional, most clients request it. If you do not wish to undertake this, we will continue in additional depth with the completely uncredentialed testing.

This is the "**Eyes-Open**," credentialed segment of the external review and seeks to identify ports and services enabled on the cyber assets within the perimeter. Our staff takes the perspective of an authorized user attempting to circumvent controls through the firewall. After the initial analysis with no credentials we will request a basic User ID and password, similar to what an employee or casual vendor might possess. Our engineers draw on information gleaned in "**Eyes-Shut**" testing and attempt to determine passwords and circumvent controls methodically as they move about the network and attempt to reach systems and applications, and document what can be accessed. This too, is typically completed from off-site.

It is this step where, when we can penetrate the network, we will also focus on:

- Other network devices
- Databases
- Operating systems
- Enterprise applications
- Other web applications
- Other areas

When the external work allows us to penetrate the City's barriers, JANUS consultants will undertake additional vulnerability testing (without denial-of-service). JANUS engineers draw on information gleaned from previous steps and use both vulnerability tools and manual simulation and exploration (not destructive exploitation) most appropriate to the task at hand (and with City guidance). This testing forms the basis for reporting on the status and state of security to reach the servers, desktops, or applications.

Internal Penetration Testing

During this phase, JANUS consultants begin additional rigorous testing. JANUS engineers draw on information gleaned from previous steps and use both vulnerability tools and manual exploitation most appropriate to the task at hand to prove the vulnerability exists. This testing forms the basis for reporting on the status and state of security from inside, both for a non-authorized user and of an authorized user who is exceeding authorities.

To begin the process, JANUS requests a short introductory session delivered by the most appropriate City staff members. This provides JANUS engineers with an overview of your methods and structure. JANUS also requests a presentation of organizational structure, overall network components, and the network/security structure in place. Also beneficial is information about your security objectives, risk tolerance/risk aversion profile, anticipated growth/needs, etc. This can be accommodated remotely. This helps us orient our testers to search for the most valuable assets. We will work with you to ensure that a wide variety of vulnerabilities are addressed, not simply those that can be discovered via scans. To do this, JANUS staff also examine the following, utilizing various techniques depending on the technology employed and using sampling:

Scanning – We will request various credentials for your network and begin by performing internal scanning to determine what additional problems we uncover, beyond those of the external work. Once we complete this step, we will move on to the following items. Various tools are utilized, depending on your needs and what is found during the scanning process. We will either work with you to utilize a VM interface or an appliance that we will send you, depending on your needs. We work with you to identify the IP addresses in scope. From this, initial scans are completed. We will determine what access we can acquire and identify the hosts, operating systems, services, servers, etc. upon which we will then perform follow-on work.

We utilize a variety of testing and scanning tools for enterprise level tests such as this. Which ones we will utilize in this project will depend on the City environment installed (please see Appendix A for a sample list of major tools that JANUS uses).

Architecture – In examining the architecture, the JANUS team determines how the network is designed, how the servers interconnect, and what the various operability functions are for each. This forms the basis for the technical analysis of the risks inherent within the environment.

Configuration – Configuration review of both the security devices and the network are some of the most overlooked, yet critical, components of security system management. JANUS, as a company that visits many different data centers every year to evaluate their system configuration elements encounters a wide disparity between sites. As a result of our work with these organizations JANUS has a great deal of experience in reviewing the configurations (and their security impacts), etc.

Target Server Business Processes – Determination of the business processes for which select servers are used. During this step JANUS gains an understanding of the relative importance of the servers to the organization. The engineers utilize this information to better target business risk and opportunities for exploitation.

Control Functions – Proposed control functions are reviewed to discern which might be at risk or allow errors. Examination of logical areas for operating platforms will involve manipulation of "other-than-regular" logical network computing paths to gain access. These paths may lead through convoluted passages and other network segments that may not be accessible initially. JANUS engineers look for other information depending on the pattern of results, and the remaining assignment requirements. Following this, a series of probing exercises is performed. These seek to determine:

- Discrepancies in actual controls vs. intended controls (per appropriate City policy and regulations);
- Weak implementation of policy according to industry security controls and best practices; and
- Security exposures that could result from the way multiple boxes are connected (particularly network routers with other boxes) or used together.

Operating System and Network Weaknesses – The next step encompasses investigation of operating system and network weaknesses related to the infrastructure (e.g., DNS spoofing), including analytical findings, recommendations, prioritization, and mitigation or closure needs. JANUS examines firewall/router ports, remote access, and services enabled to permit external access and the configuration of the internal operating systems that permit this access as compared to that recommended by the vendor (along with why variances exist). Upon completion, the JANUS consultants evaluate the implementation of the boxes, their by-pass capabilities and other vulnerabilities. (This will include your requested focus areas such as HTTP, HTTPS, SMB, ARP, FTP, SMTP, DNS, and print sharing devices, etc.).

Inter-Connectivity – In evaluating inter-connectivity, JANUS examines how the components touch the operating system, what the particular security weaknesses are, and what type of problems procedural tasks incur. Recommendations for risk mitigation are gathered.

Other areas are also tested, based both on the project plan submitted within this proposal, the RFP, and on knowledge gained from JANUS engineers' experiences at other sites. JANUS will report on exploitable processes, hosts, devices, and vulnerabilities as well as what we can get access to and their level of risk along with known fixes, recommendations, and resource estimates to correct or mitigate risk.

Depending on the specific risk, we examine how it relates to the City environment overall and what mitigating controls may be in place and operating. From this, we determine where the risk originates and how broadly it exists. Many organizations scan the IP range and identify risks that may actually relate to another location on the network or that may be false positives. JANUS' process is to investigate false positives to determine if they are real. We do not leave this to the client. While this extends the scanning process a little longer, and therefore increases the price slightly, it also eliminates significant work that the City would need to do after we completed our work if we did not take on this task. Our mission to be your partner in security requires us to perform the full service, not simply a portion of it.

As we discover and document risks, we will also be cataloguing these as to the types of recommendations that will provide solid remediation activities. This analysis is included in our risk ranking, when we determine the ease-of fix and work effort ratings.

Acceptable risk is handled by our reporting the level of the risk and what the possible solutions to it might be. You, as the business managers, must decide the level of acceptable risk that is appropriate to your specific situation. We provide you with the information on which to make that decision.

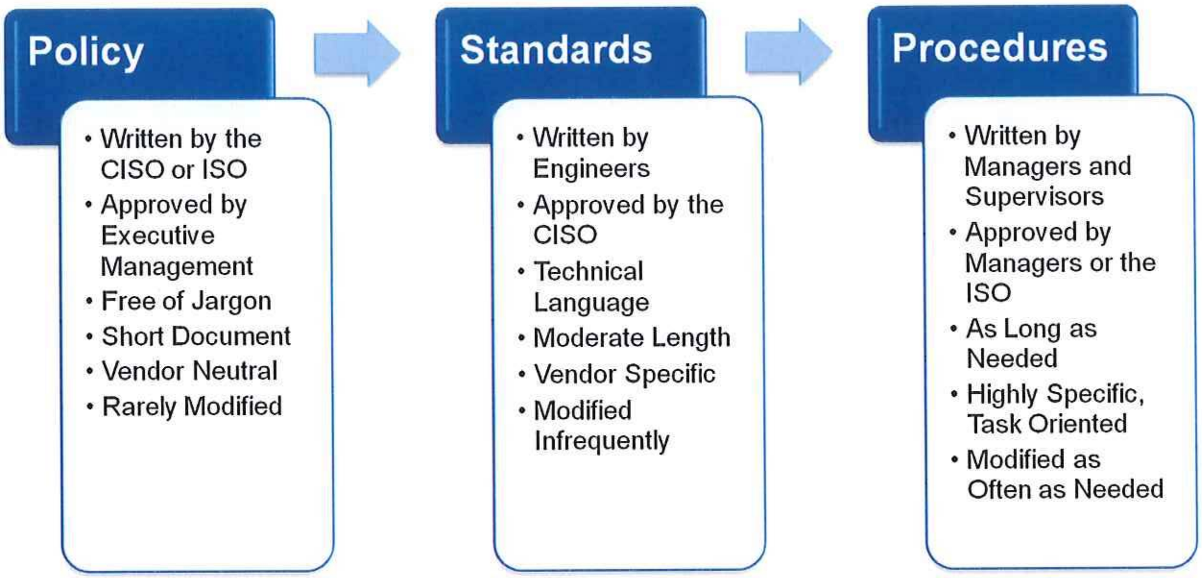
We also categorize the risks we uncover according to priority, ease of remediation, type of system, etc. We will discuss these and perform a triage that groups them into most important to least important, in our expert estimation.

JANUS assesses to all the current standards and is expert on each of them. In addition, JANUS follows our own well-established protocols to ensure a consistent process for our clients.

Governance Framework

Once an initial assessment has been completed JANUS can begin to work with the City to begin to implement or improve the governance framework that is in place.

Developing a mature security program requires a well-functioning framework of policies, standard or guidelines, and procedures upon which employees and vendors can depend and to which they must adhere.



Policy

- Written by the CISO or ISO
- Approved by Executive Management
- Free of Jargon
- Short Document
- Vendor Neutral
- Rarely Modified

Standards

- Written by Engineers
- Approved by the CISO
- Technical Language
- Moderate Length
- Vendor Specific
- Modified Infrequently

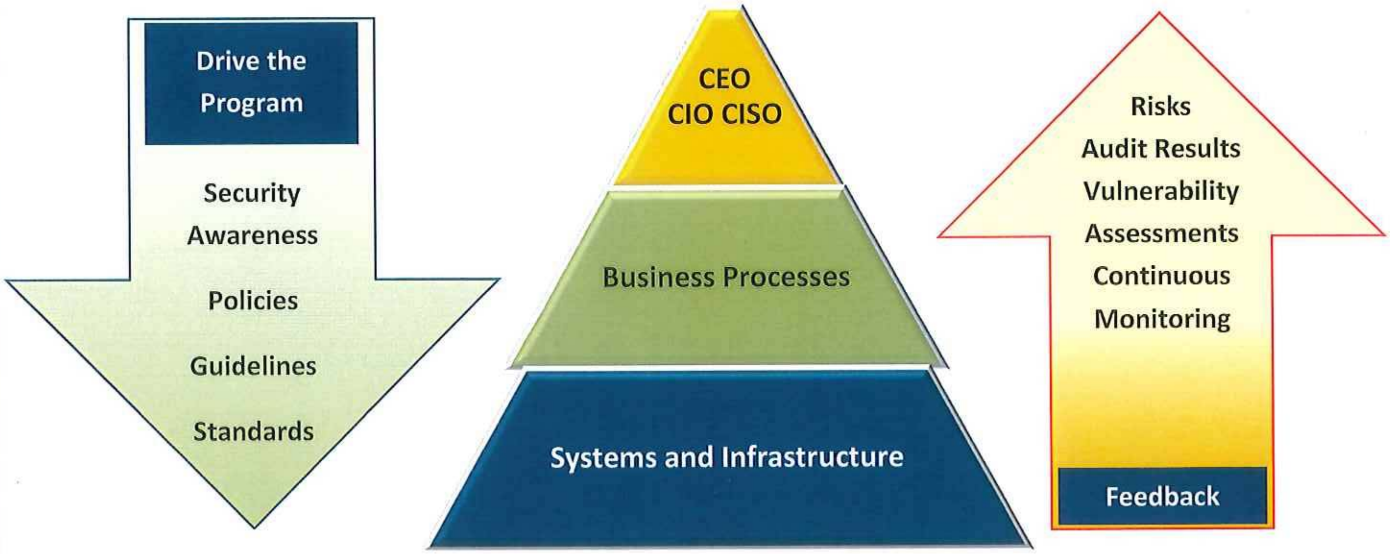
Procedures

- Written by Managers and Supervisors
- Approved by Managers or the ISO
- As Long as Needed
- Highly Specific, Task Oriented
- Modified as Often as Needed

The above figure illustrates today's leading practices methodology for developing an Information Security process that leads to good governance.

As part of our on-site assessment tasks we will analyze the governance elements and make recommendations for improvements to the City's governance program.

When this basic building block is in place and the operational practices put in place, as advised by JANUS, the City will have a major element in the overall structure of how leading practices define how the Information Security program should operate. Following this, we will advise on how the program should begin to operate, as illustrated below.



Under this structure we help develop guidance and organize it to drive the program down through the organization as illustrated in the left-hand arrow and report it back up to management as on the right side of the diagram. Structuring this continuous type of program flow results in a fully-functioning Information Security program throughout the business. This three-tiered structure is the same best-practices methodology as promoted by the U.S. National Institute of Standards and Technology (NIST) and by ISO.

Along with this, a program for adequate assurance activities can be built, including for new applications that come into production as well as the infrastructure that supports them and a strong audit function can be developed to ensure that the security program adequately protects the City. With this model, the City will then have the framework and needed operating principles. We will then work with the City and its auditors to document and help implement the needed assurance and audit type of activities that should be in place.

Policy and Procedure Review (Procurement and Risk Reporting Structures)/Develop a Five-Year Security Plan

A review of pertinent policies is a necessary component for a thorough project. To accomplish this, during the preparation phase we will request the policies and procedures that are relevant to the scope of this project and begin reviewing and assessing them for adequacy to the standards requirements of your organization (or that we assist you in developing).

This includes both the business owners and the IT staff. For the business owners, we schedule interviews to determine the interviewee's familiarity with the policies and procedures. Do they understand them? Do they adhere to them? We ask pertinent questions designed to answer these questions and to uncover information about their overall understanding.

Part of this segment of the review focuses on ensuring that, for those policies in place, staff understands how and is complying with them at all times and that they are appropriate for the environment and are implemented correctly.

We also investigate the technical aspects of policy implementation by verifying that the IT controls in place mirror the required policies and their implementation. This task takes place utilizing technical analysis of how the controls are implemented and are they in accordance with current policies and their adequacy, how they are complied with (determined during the interviews). JANUS expert observations are added regarding how the organization complies with the regulations.

During both the business process people and the IT staff (and selected managers and staff) interviews we focus on each person's understanding of his/her daily tasks (regarding policies) and how they complete them, as well as the issues they face in completing them. We will, at a minimum, address the following:

- ✓ Network user account adds, moves or changes
- ✓ Data backup procedures, schedules, off-site storage, etc.
- ✓ Server maintenance, patches, and updates
- ✓ End user desk-side support procedures, call tracking, etc.
- ✓ Network documentation procedures
- ✓ Overall Security Policies and Procedures understanding
- ✓ Any written information security plan

Along with this we will conduct a review of the organizational structure (security) and the internal resources and how these can support the proposed five-year plan – or – what changes might better support the plan.

Architecture and Operations Practices

For this task, JANUS will request up-to-date network architecture documents/drawings, including requirements documentation. We will research these documents to determine how the City's network is designed, how various elements interconnect, and the various operability functions of each. This will form the basis for the technical analysis of the potential risks inherent in each.

We will determine if appropriate levels of security are being into the architecture so that security is built-in to the underlying platform, ahead of any new development endeavors. Most architectures today should be based on a three-tier architecture model that identifies the presentation, application, and data layers that are then separated by firewalls. In order to ensure that new systems comply with that architecture, JANUS will analyze the security implications of any planned architectural design along with current documentation and schematics.

JANUS will develop section-by-section identification and track risk associated of all systems owned by City/Schools and prioritize impact.

Backup and Recovery

We will begin our analysis by examining the policies for data recovery and backup. Our focus will be on determining if, and how easily/quickly, the City could recover in the event of a breach.

During the analysis we couple the policies with the current architecture to understand if the policies would actually work and determine their weaknesses (if any) that could cause points of failure in the backup recovery operation or that might lead to a poor recovery and response result. We work with your staff to determine where the backup and recovery function resides within the architecture and how the interconnections may perform in the event of a disruption.

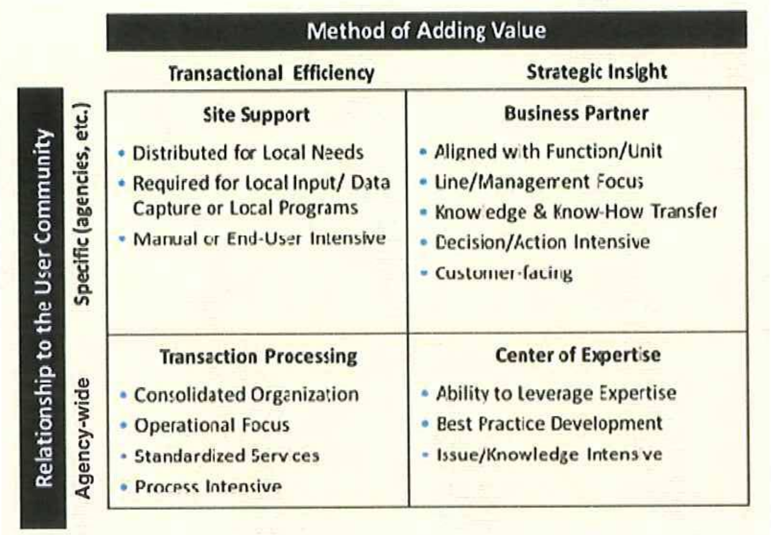
We study the documentation we receive to understand the technologies and service details needing to be utilized and to understand what additional information we need to request. We document our findings and observations as we go, continuing to factor in new information throughout the project. We also consider key aspects of the overall recoverability capability such as scalability, ability to perform as needed, component compatibility, availability and reliability, confidentiality during recovery, cost and operational factors, amongst others.

We leverage the assessment results to establish the backup/recovery needs enhancements, improvement possibilities, efficiency improvements and cost reductions, if possible. These are addressed from a 'leading practices' view and incorporate new or improved technologies that may fit within the City's strategy (or be incorporated within the strategy).

Our service delivery model evaluates each taxonomy or process component by two criteria:

1. Method of adding value; and
2. Relationship to the user community.

This fundamental structure provides a context for the dialog regarding areas in which changes could reduce costs or provide for leading practice implementation through new capabilities. This evaluation is represented in the following diagram.



Relationship to the User Community		Method of Adding Value	
		Transactional Efficiency	Strategic Insight
	Specific (agencies, etc.)	**Site Support** • Distributed for Local Needs • Required for Local Input/ Data Capture or Local Programs • Manual or End-User Intensive	**Business Partner** • Aligned with Function/Unit • Line/Management Focus • Knowledge & Know-How Transfer • Decision/Action Intensive • Customer-facing
	Agency-wide	**Transaction Processing** • Consolidated Organization • Operational Focus • Standardized Services • Process Intensive	**Center of Expertise** • Ability to Leverage Expertise • Best Practice Development • Issue/Knowledge Intensive

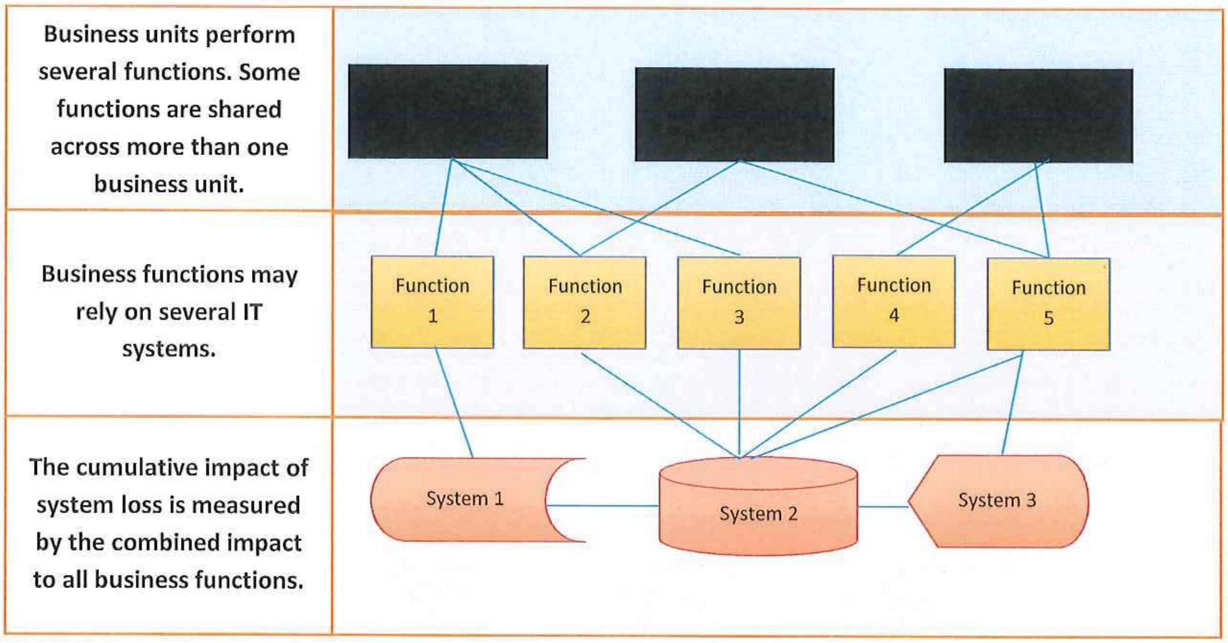
The baseline model and supporting analysis complement this evaluation and dialog. Efficiencies are estimated for the needs analysis and gaps in efficiency are used to develop a benefit realization plan. This service delivery model design works in conjunction with best-practice process design and the implementation of enabling technology to develop a complete picture of the disaster recovery process.

Quite often IT staff may have information about system usage or the track record of past outages that adds valuable insight to this process. JANUS collaborates with IT staff to understand the dependencies and relationships between systems such that appropriate policies can be developed and understood.

From our collaboration with staff the outcome of the interviews becomes threefold:

- Validate the inventory of systems and services in scope
- Identify dependencies and interrelationships between systems
- Obtain a technical perspective on the City's needs. Quite often technical staff may have unique insight into operational requirements.

JANUS assembles our findings into a consolidated matrix aligning needs with what currently exists.



Business units perform several functions. Some functions are shared across more than one business unit.

Business functions may rely on several IT systems.

The cumulative impact of system loss is measured by the combined impact to all business functions.

Association of Business Functions with System Dependencies

JANUS presents our findings to your technical team, in an open and collaborative forum. This discussion verifies our conclusions and begins the conversion about potential remediation options and plan/policy needs. JANUS also develops recommendations to close recovery gaps and mitigate identified risks. Our recommendations are developed with sensitivity to cost and practicality.

Incident Response

The effects of a data privacy breach may be wide ranging, from a relatively small amount of confidential data loss/theft, all the way to cyberattacks that attempt to seriously impact or destroy the entire business. Also worthy of consideration, the impacts can take many forms and have multiple negative image/brand consequences in addition to direct financial losses, which may include:

- Loss of public confidence
- Damage to Department's reputation
- Subsequent harm to those whose PII was lost
- Cost of recovery/remediation

There are a number of actions an organization must take to prevent or minimize the negative impacts of a data breach. Given the breadth of our experience, we can offer valued support at appropriate stages and coordinate response activities related to a breach. The first action, of course, is to build a strong security program aimed at preventing unauthorized access and safeguarding information and devices from theft, damage, and/or corruption. From our previous work with scores of clients, we understand the investments that the City may have made in secure infrastructures and strong security management activities. Even so, threats are constantly evolving and the City infrastructure is dynamic, both of which contribute to the need for "prevention." Given this ever-present situation, the next important action/capability must address "detection" of actual or suspected privacy/security breaches. There are several types of breaches that detection mechanisms must be prepared to identify, including:

- Hacking
- Theft of devices/equipment
- Phishing
- Pharming
- Malware
- Denial-of-Service attack
- Website corruption or theft
- Employee corruption, destruction, theft of data
- Social Engineering

Depending on when an incident is detected (and if it is still present and/or progressing, i.e. malware), "containment" activities may need to be launched to limit the damage. These activities typically call for the deployment of special tools and skilled technicians trained in Level 1 incident support and "first responder" activities.

After identification and containment, "investigation" is the next activity to be undertaken, to establish the extent of the damage and ascertain the causes and identify the perpetrator. This frequently requires the use of advanced digital forensic techniques and tools that can uncover events leading up to the breach and help not only to identify the origin/individual but also to recover data that are unreadable by normal means. Depending on the nature of the incident, it may be necessary to involve law enforcement agencies to ensure legal recourse and/or comply with applicable laws.

The next step in the process is "remediation" which addresses the exposures or security "cracks" that allowed the incident to occur successfully, and repairs systems and/or recovers lost or corrupted data. Again, this typically involves special skills or tools since the incident may have involved new methods or approaches not previously encountered.

The last step is typically the pursuit of remedies against the perpetrator that may take the form of disciplinary action or litigation. In order to build incident response capabilities, it is important to have a process that provides feedback, knowledge, and new information to keep the people and tools within the process as current as possible. We will work with the City to assist in building a strong Incident Response Plan.

Part of our work effort will be to assist the City to implement each of the elements that we have assessed, evaluated, and examined, as scoped in the RFP. Once we have completed the assessments, we will hold feedback sessions and from the results of those, we will develop plans for the next steps in the project.

Create a Cyber-Security Project Plan

Create a detailed Project Plan to address the vulnerabilities and risks identified in the Assessment. The project plan must incorporate the findings and results of the Assessment, determine what corrective actions, if any, are necessary to adequately protect stakeholders' interests.

1. The Plan must articulate the preventative, detective and corrective controls needed to address the vulnerabilities and risks identified in the Assessment. Controls must be specific, measurable, actionable, and cost effective. Wherever possible, controls should be tied to relevant and achievable industry standards and benchmarks against which the success of the Cyber-Security Program can be measured over the lifetime of the contract.

2. Provide recommendations to clarify job duties and responsibilities for MHIS staff for managing cyber-security and technology-related risk across all City\School systems, including all assurance and audit activities needed to ensure the successful implementation of the Cyber-Security Program. Create best practices for secure configurations of laptops, workstations, and mobile devices.

Cyber Security Plan

Upon completing the assessment, JANUS will provide a project plan that identifies the corrective actions (if needed). This will be detailed and drawn from our specific findings to provide you with measurable, actionable, and cost-effective alternatives and/or solutions. We have many years of experience in providing such results for our clients. Our assessment will identify the relevant security standard(s) that apply to the finding so you will know immediately what applies to each finding (please see samples included within this document). As part of the plan we will also study job duties and responsibilities of MHIS staff and clarify these, based on our years of dealing with IT staffs across many industries and government functions regarding cyber security.

Organizations are becoming more focused on developing metrics which can become part of the cyber security management process. These are initially developed during the governance assessment and follow-on planning phases. They will become more prescriptive as the program matures and we will help guide you through this maturation process. In addition, our technical security staff will work with your MHIS personnel to create best practices for your laptops, workstations, and mobile devices, among other areas for which you may wish to have improved practices developed.

Execute the Project Plan

Assist the City of Hartford in the execution of the proposed Project Plan, to include:

1. Project management resources to successfully execute the Project Plan, including the preventative, detective and corrective controls needed to implement the proposed plan.

2. Assist staff in developing RFPs related to the implementation of the Cyber-Security Plan; such efforts are expected to include:

a. Ensuring contracts resulting from those follow-on RFPs have measurable verification and validation tasks incorporated into the acceptance criteria so that future products and services remain aligned with the goals and requirements of the Cyber-Security Program.

b. Assisting the MHIS security staff with future related contracts to ensure the work is correctly aligned with the goals and requirements of the Cyber-Security Program.

c. Ongoing assessments and policy reviews to ensure the City of Hartford's ongoing efforts under the Cyber-Security Program remain aligned to Cyber-Security Plan.

d. Coordinating regular vulnerability and penetration tests against critical assets to identify Weaknesses in the controls and countermeasures protecting the City\School systems; to include periodic digital forensic and incident response ("DFIR") exercises.

e. Drafting updated policies, procedures and Executive Directives in accordance with evolving federal, state and local requirements and industry best-practices related to cyber-security.

f. As-needed tasks to ensure the accuracy, effectiveness and relevancy of the Cyber-Security Program in the face of new and emerging cyber-security threats.

g. Perform an additional external scan and vulnerability assessment after remediation.

3. Over the lifetime of the contract, the successful firms will support MHIS and assist staff in maintaining the accuracy, effectiveness and relevancy of the Cyber-Security Program.

Execution of the Plan

All of the items you have mentioned in this list are things that we provide regularly for our clients, including developing vendor-neutral RFPs and follow-on contracts designed to benefit the City, not the vendors. Because we are vendor-neutral, we serve only your interests.

We can regularly perform assessments and penetration tests, perform digital forensic examinations, and work with you to formulate and conduct incident response exercises.

We assume that as your program evolves, we will also be updating polices, Executive Directives, and procedures, as needed in accordance with any of today's leading standards and guidelines.

You have also mentioned additional tasks to ensure the Program in light of new and emerging threats. JANUS has one person whose entire job is to identify new threats and tools daily. We can bring that knowledge to the City and provide you with what you might need that reflects the most up-to-date thinking in the industry.

2.3.1 General

The vendor and or vendors shall provide end-to-end solutions required for Cyber Security. The solutions will include all hardware, software, supplies, installation, and integration with existing security infrastructure. The solution must include, but is not limited to, the following components and products:

- Incident and Threat Management
- Intrusion Detection/Prevention System
- Security Monitoring Tools RSA Security Analytics
- Digital Forensics
- Malware Analysis and Advanced Persistent Threat (APT) Defense
- Network Access Control
- Network Traffic Visibility and Aggregation
- Penetration Test

Please note: The proposed equipment must provide minimal disruption during hardware and software upgrades. The City prefers a solution that provides the most non-disruptive upgrades. The vendor shall provide reference to or documentation of the procedure for performing non-disruptive upgrades of both hardware and software. In addition equipment should simplify cyber security management and increase IT efficiency.

Respondents should review the *Requirements Matrix* below. For each Item, indicate whether your product meets the requirement by responding with a "Yes," "No" or "Partial". For all answers indicating partial support, please explain in the space provided. You are welcome to use the explanation box to provide additional information for "yes" and "no" responses if you believe it will be helpful in assessing your offering.

2.3.2 Requirements Matrix

JANUS' Response to Item 2.3.2 Requirements Matrix

The Requirements Matrix is focused on hardware and software that generates alerts and similar tasks. JANUS provides all the services you will need prior to purchasing hardware and software. Our function is to provide you with the framework and governance structure, understand the risks, and ensure that staff are prepared to license/purchase the best hardware/software components for the City. Tying penetration testing to a hardware/software vendor only provides you with results that lead to the specific vendor's solutions that he/she is selling – not to what is best for the City.

Hardware Requirement	Y | N | P	Explanation
Features / Functions	N/A	
Vulnerability Management	N/A	
Provision to generate automatic mail alerts	N/A	
Provision to send alerts to multiple recipients	N/A	
Licensing should be a per device and not user/IP based (should support unlimited users)	N/A	
Handle Intrusion Prevention/Intrusion Detection	N/A	

Shall be port agnostic and analyze all data on all ports all the time for applications identification to prevent evasive tactics used by modern hackers and malware.	N/A	
Prevent evasive users and applications from bypassing security functions, all product functions for IPS, Threat Prevention, and Anti-Virus, shall not require specific software port and protocol combinations for detection, mitigation, or enforcement.	N/A	
Should include a Zero-Day threat prevention system that validates executable files passing through the firewall, and provides automatic cloud-based behavioral threat analysis of unknown executables, and automatic signature creation to block delivery for executable files that are deemed dangerous by the analysis system	N/A	
Decrypt outbound and inbound SSL.	N/A	
Integrated Multi site management	N/A	
Dedicated protection for web servers	N/A	
Provide real time threat prevention	N/A	
The solution should provide protection against the increasing threat vectors and malware introduced by internet applications	N/A	
Any changes or commands issued by an authenticated user should be logged to a database	N/A	
System Availability		
At a minimum the expectations are 99.99% system availability, 24X7, 365 days per year.	N/A	
OS Support		
Windows Server 2008, 2012, 2016,	N/A	
Linux	N/A	
Citrix	N/A	
Application Support		
MS SQL Server 2008 R2, 2012, 2016, 2019	N/A	
Oracle	N/A	
Exchange	N/A	
Security		
Any changes or commands issued by an authenticated user should be logged to a database	N/A	

Password, RADIUS, TACACS, X.509, Secure-ID authentication methods	N/A	
AES 256 bit, 3DES 56-168 bit	N/A	
Reporting		
Selection of "canned" reports	N/A	
User-configurable reports	N/A	
Real-time report generation	N/A	
Export reports to .PDF, .HTML and .XLS	N/A	
Service & Support		
24x7x365 support access	N/A	
Provide updates and preventative maintenance	N/A	
Access to support personnel on first call (vs. support callback)	N/A	
Access to support forums on-line	N/A	
Remote monitoring capability	N/A	

2.3.3 Equipment Maintenance and Repair Requirements

The selected vendor shall have sufficient technical and engineering staff, as regular full-time employees, who possess and can demonstrate certification by the manufacturer for the appropriate systems. Copies of all certifications of such staff shall be provided with the response to this RFP.

The City requires that respondent or respondent's partner's technical staff or support be able to respond to any city building site when warranty support or service is required.

2.3.4 Technical Workforce

Technicians shall be stationed and dispatched from within the New England Area. Proponents shall indicate the location of the service center from which technicians will respond.

2.3.4 Technical Workforce

A portion of JANUS' management and technical staff is Connecticut-based, including in West Hartford so we can promptly respond to your needs. We anticipate that staff will be dispatched from both West Hartford and Stamford.

Deliverables

Assessment results are presented in detailed reports along with an understanding of each issue's threat to your organization or weakness. These are presented in categories of critical, high, medium or low indicators for priority. Each includes a risk classification, or criticality of the risk to the City, ease of repair and/or mitigation of the issue; degree of cost associated with remediation, and a detailed recommendation about how to deal with (or mitigate) the problem. We examine what exists to control each and develop a thoughtful detailed analysis of the problems and their solutions. Critical problems are reported immediately to management and will be reported as critical in the reports (please see Appendix B for typical form of our findings).

When appropriate, we include a Reference section following the business risk. This is where we include information about the specific standards, laws, and regulations with which you must comply that are applicable to each finding.

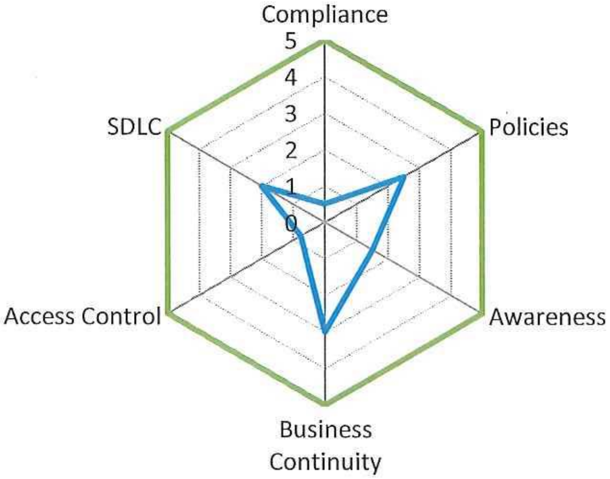
Our deliverables are submitted in draft, then final versions. Draft reports provide the needed actions, with detailed findings, recommendations, designs, or documentation and will be presented to the City for a feedback period prior to completion of the final report. After comments and review, final reports are submitted.

Our reports are prepared immediately after completing each assessment and are available within a reasonable period of time, often approximately two weeks. However, occasionally this takes longer if there are extenuating circumstances such as large numbers of findings, complex designs that require multiple feedback rounds, etc.

Assessment Draft Details

Reporting encompasses both draft and final documents. Each report includes the risks and out-of-compliance issues discovered along with detailed analysis of what was found, conclusions, and recommendations. A unique component of JANUS reports, and of significant help to management, is a definition of the business risk that each finding causes. This is great value to management for it helps it understand *why* each finding is important to the City's business in terms that are not technical. This helps translate what are often very technical results into the actual risk to the business that everyone can understand. This is in addition to the technical finding.

Beyond the business risk, the report contains proof of findings in the form of logs, screen shots, IP addresses, and any other proof that JANUS gathers during the testing period. We also work to include meaningful graphics and illustrations, such as the heat map below.



Where appropriate, we include charts and diagrams that will be meaningful. The chart above illustrates where the customer should address its focus. For the JANUS customer profiled in the example above, its policies are one of its stronger areas (a 2.5 on a scale of 1 to 5 – 5 being better) along with business continuity (a 3 on a scale of 1 to 5). Compliance with regulations, on the other hand, is very weak, so additional focus should be placed here first. Particularly in the Executive Summary, this will be very helpful.

Report Summaries

Beyond the executive summary report, we present a concise summary in addition to the technical findings in each of the reports. In this section, the management summary chart is a helpful overview. For this, JANUS works to produce a meaningful explanation of the most important elements of the assessment tasks. The following is one example of such an analysis.

#	System	Business Risk/Impact	Vulnerability Description	Solution	Risk Level
1	[redacted].org	Private history of [redacted].	A history of several years of [redacted] is stored in Google, potentially violating [redacted].	Configure the robot.txt file, and coordinate with Google and Archive.org to remove historical data.	High
2	[redacted]	Developer console in the DMZ may lead to alteration of production code and data.	The management console for the [redacted] is exposed to the Internet.	Remove administrative and developer tools from external access through the DMZ.	High
3	[redacted] [redacted] [redacted] [redacted] [redacted]	Defunct test and development websites exposed to the Internet.	Non-production websites may be un-monitored, with untested or unconfirmed security, and	Remove websites from the Internet that are not currently used for production purposes.	Medium

#	System	Business Risk/Impact	Vulnerability Description	Solution	Risk Level
			may contain production data.		
4	[redacted] [redacted] [redacted]	Websites enable user names to be guessed.	Attackers can discover valid users' names during reconnaissance prior to an attack.	Alter error messages to reveal no information during invalid authentication.	Medium

Deliverables will be submitted in draft, then final versions. The draft report will provide the needed actions, with detailed findings and recommendations, and will be presented to the City for feedback prior to completion of the final report. After comments and review, the final report is submitted.

Our reports are prepared immediately after completing the testing.

Technical Detail Report

Each report includes the risks discovered along with detailed analysis of what was found, conclusions, and recommendations. A unique component of JANUS reports, and of significant help to management, is a definition of the business risk that each finding causes. This is great value to management staff for it helps them understand *why* each finding is important to the City's business in terms that are not technical. This helps translates very technical results into business terms that everyone can understand.

Beyond the business risk, the report contains proof of findings in the form of logs, screen shots, IP addresses, and any other proof that JANUS gathers during the testing period.

It is typical in assignments of this nature that the first drafts of final reports are submitted to management for review and comments prior to finalization. The report contains screen shots and detailed information of the security issue found and includes:

- Executive summary (each technical report) for a non-technical audience
- Methodology and approach
- Positive security aspects identified (additional value)
- Matrix of vulnerabilities (technical summary)
- Detailed reporting
- Supporting detailed exhibits for vulnerabilities (as verification) when appropriate

Appendices will be included, as appropriate, including tools utilized and screen captures which are too lengthy for insertion within the findings.

We also provide additional value to our clients by supplying more pertinent information in our detailed deliverables than is typical. Each finding is explained in detail and contains the following elements:

- Business risk (potential impact to the City's business);

- Priority (severity rating which will address level of impact to the organization);
- Risk level (probability of exploitation rating);
- Applicable standard(s);
- Ease of remediation;
- Estimated work effort;
- Finding itself (the detailed description); and
- Detailed recommendation/remediation.

Both ease of remediation and business risk provide added value and will assist the City to evaluate how you can best utilize your resources to remediate the problems we uncover.

Once the City has had a chance to review the draft reports JANUS will produce the final reports.

Status Reports

Periodic status reports will be provided that focus on activities completed during the previous period and will include activities for the next period; issues and problems; project risks; and needs from the City staff.

Form of the Deliverables

We will produce all deliverables in electronic and hardcopy (if required). These can be deposited into JANUS' secure Portal for rapid and easy retrieval by the City personnel accompanied by high levels of security – or we can specifically deliver them.

Personnel

JANUS will assign individuals to this project who have participated in multiple information security projects that are similar to your request. As a result, this project will have experienced personnel to meet the requirements of the City.

Providing executive oversight will be Karl Muenzinger, JANUS' Director of Consulting. Mr. Muenzinger has extensive management experience in this type of project.

Karl Muenzinger is a Project Manager and senior consultant with deep experience in NIST, ISO, HIPAA, and IRS security standards as well as many others. He has broad technical experience and best practices in information security and business recovery throughout government and industry. With over 11 years' experience in Information Security and over 15 years' experience in Information Systems, Mr. Muenzinger's consulting emphasizes information risk assessment and management, standards/ regulatory compliance, access controls and identity management, business continuity and disaster recovery planning. He has conducted security assessments and governance analyses for a wide variety of organizations, government installations, large commercial customers, and not-for-profits. He leads complex engagements for JANUS and holds CISSP (security professional), CISA (security auditor), CISM (information security manager) certifications, and has been inducted as a statutory Member of the Business Continuity Institute (MBCI) (business recovery).

JANUS will not be utilizing any subcontractors for this project.

Note: Please see sample resumes on the following pages.

Sample Resumes

Karl Muenzinger

Function and Specialization
Project Manager

- Information Systems
- Risk Management and Governance
- IT Analysis and Strategic Advice
- HIPAA, NIST, ISO and COBIT
- Information Security
- Vendor Management
- Records Management
- Business Continuity and Disaster Recovery Planning
- Project Management

Clearance
Public Trust Level 6

Representative Clients
Centers for Medicare & Medicaid Services (CMS)
New York State Teachers' Retirement System
Commonwealth of Massachusetts
New York City

Certification(s)
Certified Information Systems Auditor (CISA) – 2009
Certified Information Security Manager (CISM) – 2004

Background

Mr. Muenzinger has over 30 years of broad Information Technology experience, which includes over 20 years in leadership roles, Mr. Muenzinger offers significant insight and real-world experience in how large, complex organizations, government agencies, and non-profit organizations perform, focusing on governance, applications, Data Centers, infrastructure, and third-party partners. He is called upon regularly by organizations to speak on IT governance and risk management, and was a lead consultant on a recent large state Current-State/Future-State/Strategy assessment completed by JANUS. He has a strong understanding of and has worked extensively using NIST, ISO, COBIT and ITIL frameworks. Mr. Muenzinger has also provided Independent Verification and Validation of online electronic signature compliance for the New York City Department of Housing Preservation and Development.

Experience

JANUS Software, Inc. (d/b/a JANUS Associates) **February 2007 – Present**
Project Manager

- Project Manager for multiple critical infrastructure assessments including electricity and water, government and transportation.
- Leads many application and infrastructure assessments for JANUS.
- Leads HIPAA compliance consulting projects for a wide array of JANUS clients.
- Provides project leadership for information testing projects for major clients.
- Project Manager for JANUS security and IV&V tasks for Integrated Justice Project for New York City.
- Manager for Security Risk Assessments and Accreditation for applications and systems of the City of New York, across a large, multi-agency environment.
- Developed role-based training on electronic records management for a large municipal government.
- Led large vulnerability assessment for major research university in the Midwest.
- Managed and produced content for an information security training program for the Centers for Medicare & Medicaid Services (CMS) as a component of JANUS' CMS training contract.
- Managed and produced content for Learning Management System contract for a Massachusetts state agency.
- Developed Business Impact Analysis and Disaster Recovery Strategy for the main Data Center of the National Institute of Standards and Technology (NIST) in Silver Spring, MD.

Certified Information Systems Security Professional (CISSP) – 2001

Member Business Continuity Institute (MBCI) – 2008

Education

B.S. – Economics/Political Science, S.U.N.Y., Albany, NY – 1980

- Produced Business Impact Analysis for a major bank in the Northeast, providing C-level executives with a business-oriented view of disaster recovery priorities and requirements.
- Developed and presented C-level executive training on how to establish and oversee information security governance and risk management programs, for several large clients and executive forums.
- Performed System Control Assessments (SA) for CMS, in compliance with standards from HIPAA, NIST 800-53, and internal CMS regulations.
- Project Manager of risk assessment teams reviewing the infrastructure and security policies and SCADA systems of power utilities, based on National Energy Regulatory Commission (NERC) standards.
- Performed risk assessment and HIPAA security compliance review of a state Medicaid agency, involving over 70 systems and applications, data classification and Privacy Impact Assessment (PIA), third party business associates, development of an inventory and diagrammed mapping of the flow of PHI through the organization, and implementation of a governance and risk management (GRC) tool.
- Project Manager for the Financial Institutions Shared Assessments Program (FISAP) security practice. Led a team of highly skilled security professionals in the assessment of financial information assets identified as "critical infrastructure" by the Department of Homeland Security.
- Project Manager for the development of ISO 2700X policies, standards and procedures for the Ministry of Finance for the country of Georgia.

Forsythe Solutions Group, Inc. **September 2002 – December 2006**
Information Security Manager

- As Project Manager for the multi-year outsourced information security program of a major Blue Cross/Blue Shield insurance provider in the Northeast, contributed to vulnerability analysis and risk/threat assessment, security architecture review, incident response, policy and procedure development. Proactively addressed project risks. Coordinated with enterprise project management office. Produced and maintained documentation on project requirements, execution, communication plans, project schedule, metrics for success, and project closeout presentations.
- Managed a team implementing Identity Management for 4500+ users, (BMC's Control SA), including the following:
  - Self-service password reset and synchronization of passwords.
  - Identification and analysis of Segregation of Duties.
  - Role Based Access Control, reconciliation and cleansing of user profiles and entitlements.
  - Business process and workflow to request entitlements.
  - Cross-platform integration on mainframe, midrange, and LAN.
- Core member of a highly visible security program, contributing to the following:
  - Vulnerability analysis and risk/threat assessment.
  - Security architecture review.
  - Incident response.
  - Policy and procedure development.

UFJ Bank (The Tokai Bank, Ltd.) **1991 – 2002**
Vice President, Information Security Officer

- Initiated a centralized information security program that reported directly to the senior risk management committee, and partnered with financial, legal, and operational risk managers to integrate information security into the bank's comprehensive risk management framework.
- Provided senior management with a consolidated view of compliance and information risk. Worked closely with Legal, Audit, and Compliance officers to conform to Sarbanes-Oxley, Gramm-Leach-Bliley and other regulatory mandates.
- Tracked progress of multiple simultaneous system upgrades on a strictly enforced schedule. Coordinated the efforts of multiple teams of highly skilled technicians.
- Represented the bank on security and IT regulatory compliance during numerous examinations by state and federal regulators.
- Information Security Project Manager for business continuity planning, 50+ disaster recovery drills, information security policy development, risk/threat assessment, incident response, firewall management, web filtering and monitoring, antivirus.

System Engineer

- System integration and support for international banking and trade reconciliation systems.

Den Norske Bank **1989 – 1991**
Lead Programmer Analyst

- Business analysis and system design.

First Automation Services **1988 – 1989**
Manager, Information Systems

- Managed staff of 15.

Evans & Company **1980 – 1988**
Manager, Information Systems

- Managed staff of ten.

Other Experience and Professional Accomplishments

Many executive training and professional conference presentations, including:

- "How to Structure an Information Security Program Without Breaking the Bank" to the Maryland Education Enterprise Consortium (MEEC).
- "Compliance Strategy: A Practical Approach to Vendor Assessment" to the International Association of Outsourcing Professionals (IAOP).
- "A Roadmap for Information Security Maturity Using ISO 27001" to the Georgian ICT Cyber Security Conference, Tbilisi.
- "Internet of Things: A Roadmap for Security Professionals" to the CMS Security Control & Update Training conference (CSCOUT).
- Many additional webinars and presentations on the security aspects of outsourcing, vendor risk assessment, cloud migration, HIPAA compliance, tools and approaches for governance, risk management and compliance (GRC).

Function and Specialization
Subject Matter Expert

- Infrastructure Security
- Networking
- Network Architecture
- Compliance
- Banking, Finance

Representative Clients
TriNovus Systems (banking networking)
Travis County District Attorney

Certification(s)
Certified Information Systems Security Professional (CISSP)
Currently working towards Certified Information Systems Auditor (CISA)

Education
B.S., Computer Information Systems, Park University, Parkville, MO (magna cum laude) – 2000

Technical Skills
Protocols: TCP/IP / DHCP / DNS / WINS / IPX / SPX / IPSec / DLC / NetBEUI NetBIOS / SNMP / VPN / PPP / PPTP / L2TP / VoIP / SIP / POP3 / SMTP / IMAP / SSH / SMB / Telnet / HTTP / HTTPS / NTP

James Carruth

Background
Seventeen years' of experience building, enhancing, and integrating highly available, secure, and compliant infrastructures. Vast knowledge base in network architectures; infrastructure builds; government compliance; network security/privacy issues; network management and monitoring systems; business continuity planning best practices; and analysis and design. Focuses on mitigating a variety of risk factors with robust Business Continuity Planning practices, adherence to SLAs, and full compliance with SSAE16, SOC 2 audit standards. Skilled in working in regulated environments to safeguard client assets, sensitive data, and critical business systems to protect from intrusion, data corruption, and loss.

Experience
JANUS Software, Inc. (d/b/a JANUS Associates) **July 2017 – Present**
Senior Technical Consultant

- Managed Texas client security assessment.
- Network architecture compliance advisement of client institution.
- Performs compliance assessments for wide variety of clients.
- Analyzes networks and works with IT departments to improve security architecture and environment.

TriNovus Systems, Lubbock, TX **February 2005 – July 2017**
Network Services Director
Recruited for position and brought on board to mature an infrastructure that was not well structured and lacked full disaster recovery capabilities. Lead a team of up to 5 members in the build, management, and support of a high availability, core processing data center infrastructure for banking clients, who have no tolerance for unexpected downtimes.

- Managed networks and systems for a heterogeneous environment comprised of VMWare, Windows, Linux, Mac, and IBM iSeries systems. Experienced in vendor and contract management, and product research and evaluation.
- Created a technology and capability Roadmap for the execution of a well-defined strategy plus the tactics and timelines to implement that strategy. Addressed such issues as the replacement of depreciated systems, vulnerability remediation, and compliance with encryption standards and regulations.
- Within a highly-regulated industry, managed compliance and auditing work related to FFIEC, OCC, FDIC and Texas State Department of Banking oversight and SSAE16, SOC 2. Areas included business continuity planning, disaster recovery testing, vendor management, Active Directory management, patch management, anti-virus management, 3rd party software patch management, intrusion detection/ prevention systems, external penetration testing and remediation, internal vulnerability scanning and remediation and network file system segregation.

Access Control: RADIUS / LDAP / RSA / DUO

Encryption: Bitlocker / PGP / VeraCrypt / AxCrypt

Network Access & Peripherals: Secure Access Gateways · Web Proxies · Spam Filters - Print Servers; Proxy Servers · Switches · Routers · Bridges · Wireless Access Points · Patch Panels · Copper & Fiber Optic Cabling · Equipment Closets · Thin Clients

Operating Systems: all Windows clients and servers; Journaled, Raw File Systems (FAT/FAT32/NTFS/Ext2/Ext3); Novell NetWare 6.x; Linux (Debian derivatives); DOS Command Line/Scripting; Windows Power Shell; VMware ESX Server

Software: Microsoft - Word, Access, PowerPoint, Excel, Works, Outlook, Active Directory, SMS, FrontPage, Project, IIS 5.0/6.0/7.0; Miscellaneous: Mail Enable - Network health and event monitoring · Remote Access · Malware Protection: Norton / McAfee / Trend Micro / Kaspersky / Sophos / F-Secure / Webroot

- Based on successes building friendly and professional relationships, worked closely with clients to determine thorough understanding of needs upon which to determine success, and complied with quality management and continuous improvement standards.
- Developed team competencies in network and system troubleshooting, software distribution and updates, router and domain name management, performance monitoring, error validation, and support practices.
- Provided application management support focused on network security, resiliency, business continuity, and disaster recovery. Deployed enterprise class solutions for Internet and email proxy appliances, firewalls, WAN link resiliency, and network infrastructure.
- Defined and executed a Disaster Recovery and Business Continuity Plan for an infrastructure that supported 32 financial institutions.
  - Implemented BGP and autonomous system routing, allowing customers greater access to SaaS services in the event of a communications failure with primary vendor.
  - Created a production environment capable of near time local replication and daily replication to primary DR site, utilizing VMWare and 3rd party VM centric tools. The current robust environment is tested twice yearly with customer participation.
- Virtualized environment on a limited initial budget to progressively piece together the backbone of VMWare environment. Consolidated the most critical systems to just ten servers, resulting in a simplified support model with lower costs, as well as horizontal scalability as needed.
  - Expanded VMWare environment to include 70 percent of production systems, with an established DR location.
- Performed IT consulting for community banks, providing everything from building public websites, hosting email domains, and managing DNS to supporting servers, desktops, printers, routers and firewalls. Provided services for 13 banks.
- Deployed an open source tool (Nagios) as an "up/down" network monitor to alert when production, disaster recovery and customer managed systems became unresponsive.

Travis County District Attorney, Austin, TX **April 1993 – February 2005**
Senior Network Analyst (January 2001 – February 2005)

Provided technical support for an IT infrastructure distributed across three locations for a state government office with 300 employees.

- Led two network analysts in the maintenance and support of a heterogeneous network environment comprised of a high availability NetWare 6.5 cluster, Linux, Windows, and IBM AS400 systems.
- Created numerous Crystal Reports using data derived from the County's criminal justice system for such purposes as case load management, recidivism rate tracking, victim/witness tracking, and correspondence, among others. Delivered reports via the web.

Senior Financial Analyst (April 1993 – December 2000)

Budget Manager and Principal Accountant for Public Integrity Unit, a state funded prosecution department of the Travis County District Attorney.

Other Experience and Professional Accomplishments

United States Marine Corps, Jacksonville, NC **April 1987 – April 1993**
Sergeant, Active Duty Military

Mohsan Farid

Function and Specialization

Subject Matter Expert

- Information Security
- Penetration Testing
- Security Assessments
- Web Application Testing
- Firewalls
- Tools

Clearance

Department of Defense, Secret
Department of Homeland Security, Secret
Department of Interior, Secret
Department of Treasury, Secret

Representative Clients

Department of Defense

Certification(s)

Certified Information Systems Security Professional (CISSP) – 2008
Federal Information Technology Security Professional (FITSP-A) – 2010
Certified Ethical Hacker and Countermeasures V6 (C|EH) – 2010
Certified Secure Software Lifecycle Professional (CSSLP) – 2009
Certified Network Defense Architect (C|NDA) – 2011
Certified Expert Penetration Tester (CEPT) – 2012
Certified Security Analyst (E|CSA) – 2010

Background

Mr. Farid has 15 years of technical, security, and customer service experience within government and commercial industries. He currently uses his technical experience to develop, test, and engineer security assessments for various DOD and commercial entities.

Experience

JANUS Software, Inc. (d/b/a JANUS Associates) **February 2017 – Present**
IT and Security Consultant

- Performs security scans, analysis, and penetration tests of client networks and operating environments.

Pervade Security **June 2013 – February 2017**
Penetration Tester

- Performed mobile, internal, and web penetration testing for various clients.
- As a pen tester for the IRS Penetration Test Code Analysis team, responsibilities included: managing all aspects of assessment and response engagements from launch to completion.
- Internal/external penetration testing, vulnerability assessments, and web application penetration testing.
- As a mobile security penetration tester for various clients, responsibilities included testing mobile applications and platforms such as IOS, Android, Windows Mobile, while leveraging the OWASP Mobile Top 10.

Vector Detectors **December 2012 – June 2013**
Independent Security Consultant/Cofounder

- Provided security consulting services ranging from internal/external penetration testing, vulnerability assessments, and web application pen testing.

Knowledge Consulting Group **March 2012 – December 2012**
Senior Penetration Test Engineer

- Internal/external penetration testing, vulnerability assessments, and web application pen testing.
- Led pen testing engagements in support of the KCG Cyber Attack & Penetration Division for customers such as Rapid7, Akamai, Stratfor, Intelligence, MetLife, DC WASA, Empire State NYC, BPD, DHS, DOI, FMS, and FRB.
- Conducted ST&E for federal information systems in accordance with NIST standards and oversaw and managed the delivery of security assessment services to commercial and federal customers.
- Led the FedRAMP initiative as a 3PAO technical lead for Akamai.

Licensed Penetration Tester (LPT) – 2011
Certified Penetration Tester (CPT) – 2012
Qualified Ethical Hacker (QEH) – 2011

Education

Bachelor of Science in Business, Virginia Commonwealth University

Technical Skills

<u>OS/Applications</u>: Windows, OS X, Linux: Redhat Enterprise, CentOS, Debian, Kali Ubuntu, Fedora, Suse, Slackware, Mandrake, Enigma, Red Hat, Beehive, Knoppix STD, NST, BackTrack, Samurai, VMware ESXi Unix: Solaris, FreeBSD/Open BSD, Open VMS, Novell

<u>Forensic Software</u>: Autopsy, SleuthKit, dd/dc3dd, PTK, DD, Pasco

<u>GOTS Scripts</u>: DISA Unix SRR, Oracle SRR, SQL SRR, WebSRR, and Gold Disk

<u>Penetration and Vulnerability Scanning Software</u>: Metasploit, Responder, Core Impact, Nmap, Nessus, AppDetective, ISS, FoundStone, WebInspect, Retina, Nikto, NTOSpider, SuperScan, Netscan, Retina, X-Scan, AIX, Unicornscan, Sshmitm, Webmitm, Arpspoof, Hydra, Cain and Abel, TCP DUMP, Netcat, Cryptcat, Hping, Xscan, AutoScan, Firewalk, DNSwalk, Fport, HttpPrint, Immunity Canvas, OpenVaus, admsnmp, Cisco Global Exploiter, Fierce, Maltego, Mantra, SQL Ninja, snmpenum, onesixtyone, Armitage, Karmetasploit, Social Engineering Tool kit (SET), WCE Windows credential editor,

- Managed all aspects of assessment and response engagements from inception to completion.

Telos Corporation — **February 2008 – March 2012**
Senior Security Engineer

- Conducted vulnerability assessments, penetration testing, and web application assessments. Performed multi-scaled analysis ranging from large scale vulnerability to automated and manual penetration testing in addition to web application testing. Vulnerability assessments are in accordance with the Department of Defense.
- Information Assurance Certification and Accreditation Process (DIACAP, DITSCAP, AR 25-2, and NIST SP 800 series).
- Managed all aspects of assessment and response engagements from inception to completion.
- Leveraged the Application Security and Development Security Technical Implementation Guide and OWASP to provide security guidance for use throughout the application development lifecycle.
- Provided the guidance needed to promote the development, integration, and maintenance of secure applications.
- Utilized VMware ESXi server to develop a lab environment for application security and penetration testing.
- Leveraged multiple tools in Back Track distro to perform penetration testing and web application testing.
- Performed vulnerability testing leveraging tools such as Defense Information System Agency (DISA) Security Readiness Review (SRR) scripts, Nessus/Newt, AppDetective, NTO Spider, Nikto, ISS, FoundStone, and WebInspect.
- Consolidated and analyzed the output from the findings tools and presents them in the form of a vulnerability matrix consisting of a POA&M, DIP, SIP, and DIACAP scorecard.

Security University — **August 2010 – December 2010**
Intern

- Immersed students into an interactive environment where they were shown how to scan, test, hack and secure their own systems. The lab intensive environment gives each student in-depth knowledge and practical experience with the current essential security systems.

IntelliDyne, LLC — **October 2006 – February 2008**
Security Engineer

- Performed vulnerability assessments and application testing in accordance with the DoD Information Technology Security Certification and Accreditation Process (DITSCAP).
- Responsible for evaluating application security within the Software Development Lifecycle (SDLC) of clientele.
- Assisted in the design, development, testing, deployment, and maintenance of secure applications.
- Evaluation of system documentation such as System Security Authorization Agreements (SSAA), Security/System Design Documents (SDD).
- Conducted technical interviews with developers and program security personnel.

Nexpose; Browser exploitation framework, Mimikatz

Sniffers: Ethereal, Etherape, Ettercap Wireshark, Dsniff, Kismet, tcpdump

Debug/Reverse Engineering: Peach Fuzz, FileFuzz, !Exploitable, DebugDiag, Spike, Immunity Debugger, IDA Pro, Ollydbg, windbg

Web Application: Burp Suite Pro, SQLMap, AppScan, ZAP proxy, Tamper Data, Acunetix, Paros, WebScarab, w3af, Wfuzz, WebInspect, Nikto, NTO Spider, Net Sparker

- Developed detailed test plans for identifying the system accompanied by its components, security requirements, in addition to testing methodologies and tools.
- Facilitated negotiations with all Points of Contact (POC) for system testing in order to establish testing time, location, and to provide those who were tested with an understanding of what to expect during the auditing phase.
- Performed vulnerability and application testing using tools such as Defense Information System Agency (DISA) Security Readiness Review (SRR) scripts, Nessus/Newt, AppDetective, ISS, FoundStone, WebInspect, John the Ripper, Nmap, and Cain and Abel.
- Consolidated and analyzed the RAW data from the findings tools and presents them in the form of a vulnerability matrix with recommendation for mitigation or elimination of the identified risks for both technical and managerial audiences.

AcquireSoft **April 2002 – October 2005**
Technology Officer

- Managed a team of engineers in Information Security evaluation, design and implementation of AcquireSoft's technical infrastructure.
- As the director of the AcquireSoft Risk Management process, performed regular data hygiene activities in addition to creating and administering internal and client databases.
- Responsible for the development and maintenance of the IT Audit mission, strategy, procedures, secure application development, and risk assessments.
- Secure application development conducting code reviews for security flaws for various customers.
- Trained developers on secure development standards.
- Assisted development teams with their information security/information assurance concerns.
- Performed routine data encryption for internal security purposes along with clientele data, and installed and configured ERP solutions.

Item Inc. **April 2000 – December 2002**
Systems Engineer and Sr. Network Administrator

- Designed, tested, and implemented systems that focused on the infrastructure components. This included network switches, routers, LAN/WAN connectivity, remote access, Windows NT and Active directory domain design and implementation, network management design and implementation.
- Performed network security/information assurance activities including active audits, firewall, and Intrusion Detection System (IDS) configurations.
- Exercised defense in-depth by utilizing multiple layers of security.
- Responsible for installing and maintaining networks on-site and off-site. In this capacity duties included the configuration of client systems including server and workstation operating systems, configured customer databases to custom specifications to best meet needs, and performed upgrades to products with optimum security settings/permissions.

RCN Internet **May 1999 – March 2000**
Help Desk Support

- Analyzed and diagnosed Internet and operating system related errors while providing client with superior customer service.
- Exceptional skills in problem solving and diagnostics.

	• Removed Internet related viruses through dos, connecting into mail servers, troubleshooting modems, installing and re-installing drivers, com ports, configuring receive and transmit buffers, communicating and running diagnostics, and resetting modems with initiation strings. • Performed advanced operating system trouble shooting such as extracting Winsock's and manually uninstalling DUN, manual repairing and uninstalling IE 4 and 5. • Edited registry settings, scanning critical system files and replacing them if they were corrupt. • Optimized Internet connections; power cycled cable modems and tweaked registry settings for optimal performance.