JANUS
ASSOCIATES

Proposal for:
IT Security Assessment

Solicitation Number: 6100028378

Prepared for:
Commonwealth of Pennsylvania

April 11, 2014

JANUS Software, Inc.
d/b/a JANUS Associates, Inc.
1055 Washington Boulevard
Stamford, CT 06901
203-251-0200
Contact: Patricia Fisher
PatriciaF@janusassociates.com

Table of Contents

JANUS
ASSOCIATES

April 11, 2014

Mr. Dan Paese
Enterprise Information Security Office
1 Technology Park
Harrisburg, PA 17110

Dear Mr. Paese:

JANUS Software, Inc., d/b/a JANUS Associates (JANUS) is pleased to present the Commonwealth of Pennsylvania, Office of Information Technology, Enterprise Information Security Office (Commonwealth) with this proposal to provide an IT Security Assessment.

Since being founded in 1988, JANUS has focused on providing leading edge Information Security services and has extensive experience in performing security and penetration testing assessments of the type requested by the Commonwealth. JANUS regularly provides similar services for federal, state and local government entities, private sector businesses; and not-for-profit organizations. Examples of recent similar projects include the Commonwealth of Massachusetts, the State of Wyoming, New York State, and the State of Maryland Comptroller's Office.

In addition, JANUS has extensive experience in conducting technical risk analyses of a variety of web applications and has been specializing in these since they began to be offered on the Internet. Over this period, JANUS has 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, 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 any tools, or vendor offerings.

Thank you for offering JANUS the opportunity to submit this proposal. Our offices are close to your locations, our staff is ready to begin, 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,

Pat[redacted] Fisher
President & CEO

Understanding the Problem

Provide a brief narrative that accurately assesses the problem to be solved based on your understanding of the project requirements stated in the SOW.

This project requests:

1. External testing services of the OA/OIT environment providing enterprise services to the Commonwealth agencies. These external services include both an analysis of what information might be available via the Internet that could help an attacker gain entry to OA/OIT networking elements.
2. Focusing on the external footprint discovered, complete scans that provide information of what is possible to reach within the network. From this, determine what particular issues this access causes, document these in detail, their criticality, with detailed recommendations for mitigation or remediation. Within this task an examination of web applications is included where JANUS will search for vulnerabilities, particularly of the OWASP Top 10 problems.
3. An on-site visit to provide a wireless security assessment and penetration test at 2 locations in Harrisburg.
4. An on-site executive management presentation following completion of the work.
5. Project reports including:
    a. External scan report including documenting all assets.
    b. All assets that contain web applications along with a list of pages that were crawled through.
    c. A report detailing JANUS' methodology, findings, severity, and recommendations. JANUS provides additional information in its reports that will be discussed in a later section.
    d. A similar report for the wireless test.
    e. A high level executive report with a summary of findings, inclusions, and recommendations in PowerPoint format.
6. Management and governance reports including:
    a. JANUS' Task Plan: JANUS provides this in MS Project for all its clients.
    b. Weekly Status Meetings: This will be formalized with an agenda and written results prior to the status meeting, then finalization after the meeting.
    c. Issue Identification: JANUS anticipates including this in the weekly status meetings to ensure that problems are quickly addressed (critical items or issues are brought immediately forward) and so that resolution can be made part of the formal project record. If OA/OIT desires a separate report, JANUS will produce these.

JANUS will now describe our methodology for achieving the above.

Methodology

JANUS focuses its reviews on risk-based assessments. This is the method that regulators are rapidly moving towards; however, JANUS has been working with its clients utilizing risk management techniques for many years. What this means is that security components must reflect 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. Thus, a second important component of a risk-based vulnerability assessment process is the risk acceptance component. That is, providing you with information and advice so that you can determine which risks you might be able to live with, and those risks with which you are not willing to live.

As a part of its regular assessment process, JANUS:

- *Identifies* specific threats and risks to an organization;
    - To understand the actual risk to the organization posed by the specific vulnerabilities
    - Test the security of the environment (network, servers, applications, etc.)
    - Determine if current security measures are actually detecting or preventing potential attacks
- *Recommends* actions for mitigation;
- *Assigns* a “risk rating”;
- *Calculates* the effect of the threat or risk;
- *Documents* the problems; and
- *Prioritizes* findings by the damage the organization might sustain if the vulnerability was exploited.

While our risk and vulnerability assessments include known vulnerabilities and 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 and are examined carefully to determine the likelihood of exploitation by past and present employees, and other users. However, the ability for authorized individuals to circumvent processes is also a major focus area where analysis also will occur.

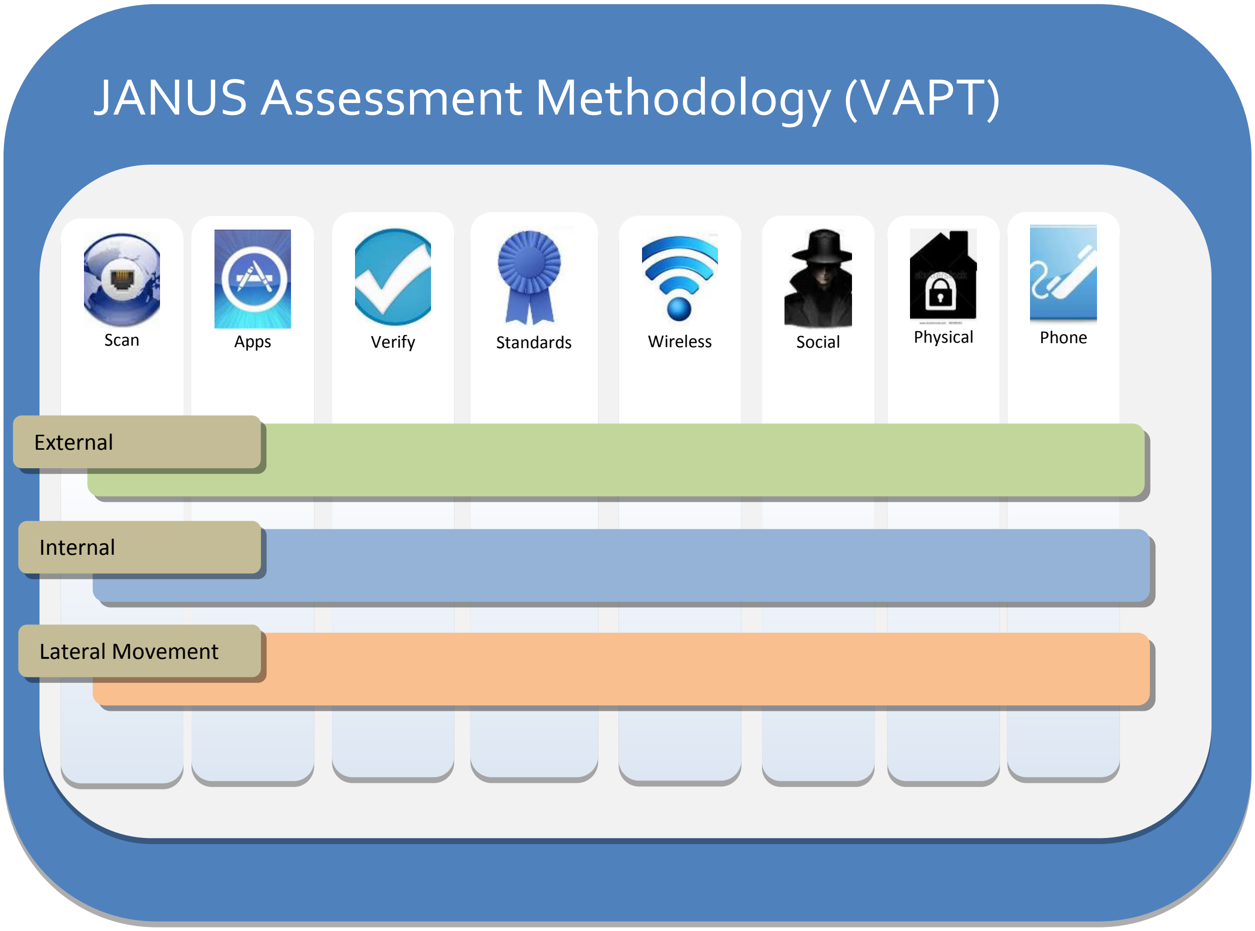
1 *Preliminary Activities*

As soon as possible after the contract award has been communicated, a project kick-off meeting is scheduled. The kick-off can be conducted via teleconference. During the kick-off meeting the following items are typically covered:

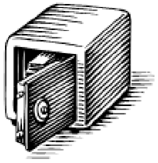
- Review terms of the project;
- Verify project scope and deliverables;
- Arrange for necessary access permissions (if any);
- Arrange for letters authorizing the tests (to be carried by JANUS consultants at all time during the testing);
- Review the work plan to finalize the timing of external tests, on-site visits;
- 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 JANUS (if any);
- Introduce Commonwealth and JANUS 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 testing plan that is designed to offer consistency and thoroughness, we will produce this documentation during the earliest phase of the project. This will be discussed with the Commonwealth to ensure its focus and accuracy.

JANUS' assessment methodology, which we term our Vulnerability Assessment and Penetration Test (VAPT), consists of the following elements. These are categorized within groups and described throughout this document. However, the Commonwealth has not requested all the eight services contained in a full VAPT; therefore, those sections have been excluded (social, physical, phone).



This project will focus on the external elements of a security assessment.



External Assessment - View of the Environment through the Internet

We will conduct focused external security testing of the public network infrastructure devices/systems to identify ports and services enabled. In this testing, JANUS consultants seek to gain as much knowledge as they can about the Commonwealth and its Internet presence using resources available to any technical person via the Internet.

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 Commonwealth. 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/E-mail server(s)
- Other devices identified during testing

It should be noted that testers might veer from their 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

The Commonwealth has requested what JANUS terms its "**Eyes-Shut**" testing approach. This means that JANUS performs a thorough examination, beginning with scanning, from outside, through the Internet with no Commonwealth originated User-IDs or information (if the Commonwealth wishes to extend the project with low level IDs JANUS can also accommodate this need). The "Eyes Shut" approach is described below. Potential target hosts are identified and screen prints 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, USERIDs, 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, 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 for potential weaknesses, and assess the resiliency to malware and malicious code.

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. 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 will report this information in our deliverables. To prevent being blocked from testing, we will work with those Commonwealth 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 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 penetration 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.

Network Scans

JANUS uses a variety of commercial, shareware, and freeware tools to conduct its penetration testing and security assessments. The following list of tools reflects those programs that have received thorough review and are frequently used by JANUS consultants. However, other tools and programs are being reviewed and explored at all times, and it is not unusual for other carefully scrutinized tools to be used in support of client requirements. In particular, there are literally hundreds of tools that are vulnerability specific (such as msadcs.pl for taking advantage of the Microsoft IIS msadcs vulnerability), and are not covered in this list. All tools used by JANUS are tested in a laboratory environment and receive a thorough review prior to their use on a client site.

Network Mapping Tools

Nmap (freeware) - This is the primary tool used by JANUS for port mapping. It supports ping scanning (determine which hosts are up), many port scanning techniques (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).

Hping2 (freeware) - This is a ping-based program that is used to send customized and arbitrary TCP and UDP pings to remote hosts and networks. It is used both to gather raw fingerprint data and can be utilized to provide "TCP specific firewalls," and other functions particularly useful for examining firewall rules.

Nemesis (freeware) - This is a command line based packet-forger that is used to create arbitrary TCP, UDP, ICMP, OSPF, RIP, IGMP, ARP, and DNS packets to arbitrary hosts and ports. JANUS uses nemesis to develop a blind spoof that sends forged packets to a target host to simulate a TCP session with a trusted platform without receiving any replies.

Sniffers and Packet Analysis

WireShark - 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. WireShark is a freeware project that attempts to emulate commercial quality analyzers such as NAI's Sniffer Pro, and is capable of analyzing real-time captures and stored sniffer traces in multiple different formats. It can also track and display both sides of a TCP session.

Shomiti Surveyor (commercial) - This is a reliable, flexible network sniffer that is used as an alternative to WireShark. It is used on Windows platforms being used for packet analysis. It can also be used to generate arbitrary packets for testing purposes.

Vulnerability Scanners

Nessus. This is the primary vulnerability scanner used by JANUS. Multiple security checks are coded as external plug-ins, thus allowing the product to be upgraded, maintained, and modified on the fly.

Whisker. This is an extremely flexible (script-based) and thorough cgi scanner that includes IDS-spoofing capabilities and anonymous proxy capabilities.

Cerberus Internet Scanner. This is a vulnerability scanner primarily used for its capability to get information from open NetBios ports (it was previously called NTInfoScan) on Windows machines.

Saint. This gathers as much information about remote hosts and networks as possible by examining numerous network services and potential security flaws. The collected data is then analyzed using a simple rules-based system. In Exploratory Mode, SAINT will examine the avenues of trust and dependency and iterate further data collection runs over secondary hosts.

SARA. This is a third generation security analysis tool that is based on the SATAN model.

Password Crackers

John the Ripper. This is the fastest and most comprehensive password cracking tool used for UNIX passwords.

L0phtcrack. This is the fastest of the Windows password crackers, and can be used to crack a dumped SAM file, the registry, or sniffed SMB packets containing both LANMAN and NT hashes.

Other System Tools

Kali Linux: From the creators of BackTrack comes Kali Linux, the most advanced and versatile penetration testing distribution ever created. BackTrack has grown far beyond its humble roots as a live CD and has now become a full-fledged operating system.

MetaSploit Pro: Closed-loop Vulnerability Validation, Phishing Simulations & Social Engineering, Web App Testing, Automation through Wizards, Task Chains, MetaModules, Out of the Box and Custom Integrations through API

Netcat: This is a network utility usable on both NT and UNIX machines to provide arbitrary TCP and UDP connections. It is often nicknamed "the Swiss army knife of network tools." JANUS consultants use this tool to provide network connections for numerous different attacks.

NT Resource Kit: This is the supplementary kit provided by Microsoft for attempt to crack most known UNIX password hashes. Cracking rules can be generated based on arbitrary word dictionaries and password patterns.

Lateral Movement and Pivoting Within the Network

Once the initial external scans are complete, JANUS will focus on examining the vulnerabilities applicable to each target. This is an important element of the security program since once an attacker gains access to a device within the target network, the attacker will certainly explore that device for information. These people are looking for information that can either be sold, or used to further the attack to meet some other goal. In many cases the attacker will install hacking tools on the compromised machine and use those tools to attack additional machines on the internal network. This process is known as lateral motion or pivoting. Pivoting has become a standard tactic of all hackers performing today's sophisticated attacks. By pivoting within the network, the attacker bypasses perimeter firewall policies and can execute attacks that would not be possible from outside the network. Pivoting attacks often go unnoticed due to their nature and the fact that they originate from within the network. By time they are noticed, it is often too late to prevent them; the attackers will have achieved their goals which may include stealing or corrupting data, deploying additional malware, hiding or opening more backdoors.

In addition, in a recent briefing of law enforcement and approved security consultants to which JANUS was invited, according to a study by a leading security research organization, once attackers utilize this type of attack organizations are far more prone (close to 100 percent) to subsequent attacks unless they understand what has happened and monitor regularly for signs of repeated activity. As a result, this type of assessment is very important.

Unfortunately, most security testing firms utilize publically available malware with real weaponized payloads as part of their lateral testing process. This malware is available in the wild and has been developed by anonymous sources. Using this sort of tool may itself present additional risk due to the fact that its origins are unknown. Additionally, it may hide the real motives of the author, potentially exposing internal resources to additional risk. With our goal of always protecting our clients, JANUS only utilizes commercially available testing products for pivoting, or products specifically designed for our clients by JANUS developers and which have been thoroughly tested.

For this component of the testing, JANUS will conduct sophisticated vulnerability testing designed to determine what can be reached within the network as approached from the Internet by using lateral testing techniques. In this extended testing, we may ask the Commonwealth for additional access at a low level, similar to what an actual low level user might have, to further examine important possibilities. While this is not required to produce the results within the solicitation, if desired, JANUS will work with the Commonwealth to exceed expectations on this test component to provide greater value.

Applications

Finding all web applications within the Commonwealth's assets as determined from an external assessment will be handled by carefully inventorying what was found, identifying specific application components, and documenting what they are as well as what we undertook to find them.

In this, JANUS will crawl through the web applications to determine what might be available via the Internet. We build upon the data collected and derived in the previous phases to refine and clarify what is found, where it is found, how available it might be from the Internet, and possible paths of attack.

Manual Verification

Manual verification is an essential component of all penetration tests, 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 Commonwealth form action plans for remediation.

Standards

The Commonwealth has asked that either NIST or ISO 27002 be utilized as the standard against which findings and recommendations are made. JANUS has significant experience in both and suggests that NIST, which is more granular, be the primary standard utilized since it will provide greater insight on the specific control recommended and will provide better clarity for the Commonwealth staff who will need to remediate findings. JANUS will also, if requested, map these to ISO for the Commonwealth's use.

From this, the Commonwealth will have the standard/guideline to which each problem relates and may choose to utilize either, or both, at its discretion thus making its regulatory compliance tasks simpler over the long term. Where Commonwealth "best practices" are found, these will also be identified.

Wireless Security

Wireless access points have become ubiquitous. With city parks and Starbucks now advertising hot spots where wireless connectivity can be initiated, the ability to control wireless access has become paramount. JANUS focuses not only on wireless connectivity itself, but also how to better secure it. With increased ability of network access for workers, wireless networks also increase the ease by which hackers can compromise the system. Even if an intruder cannot access the site network due to access control mechanisms on wireless access points, he/she can still use a wireless network card to listen to (sniff) unencrypted wireless network sessions. Security of wireless initiatives is still relatively young. The simplest solutions rely on a private key that is shared between the wireless access point and the mobile station to encrypt sessions. This key is usually in the form of a password that must be entered to initiate communication with the wireless access point. A problem arises because there can be only one key per wireless access point. In this configuration, everyone using the wireless network must know the “private” key. Obviously, this private key will not be private for very long.

Stronger security measures for the general marketplace in an unclassified setting are beginning to emerge. JANUS finds that where there is adequate rigor in installation these measures are proving useful to discourage simple wireless development from springing up. However, because it is so simple to construct our clients must be constantly vigilant to manage the wireless capabilities available. JANUS uses its expertise to assist clients in both determining how to deliver needed wireless services and also in managing the access control requirements of this burgeoning capability.

JANUS utilizes a variety of tools for its wireless testing. These include:

- Network Stumbler – identify protected and/or unprotected wireless LANs
- Kismet – detect wireless networks
- Wellenreiter – discover wireless networks, decode DHCP and ARP traffic, capture wireless traffic
- WaveStumbler – map wireless networks
- APSniff – capture wireless network traffic
- Ethereal – capture, decode, and analyze wireless traffic
- THC-Rut – access wireless access points, spoof DHCP, BOOTP, and ARP requests
- AirSnort – recover/crack WEP encryption keys
- WEPCrack – recover/crack WEP encryption keys

The Commonwealth has indicated that, for this project, it wishes to have two locations tested (1 Technology Park and 5 Technology Park). For the results of this task, JANUS will identify specific issues along with the approximate wireless network location, SSID, and WEP-enabled status. As part of the testing, JANUS will include attempts to compromise the wireless networks from outside the physical perimeter of both locations. The wireless security test will follow NIST SP800-115 guidelines.

DELIVERABLES

Testing results are presented in detailed reports along with an understanding of each vulnerability's threat to the organization; presented in categories of high, medium or low indicators for priority. Each includes a risk classification, or criticality of the risk to the Commonwealth, ease of repair and/or mitigation of the vulnerability; degree of cost associated with remediation, and a detailed recommendation about how to deal with (or mitigate) the vulnerability. We examine what exists to control each vulnerability and develop a thoughtful detailed analysis of the problems and their solutions.

Deliverables will be submitted in draft, then final versions. The draft reports will provide the needed actions, with detailed findings and recommendations, and will be presented to the Commonwealth for feedback prior to completion of its final report. After comments and review, the final report for each task is submitted (please see Appendix C for typical form of JANUS findings).

JANUS typically reports its findings regarding priority as High, Medium, and Low risk. Critical problems are reported immediately to management and will be reported as Critical in the reports, if requested.

When appropriate, JANUS includes a Reference section following the business risk. This is where we typically include reference to the specific standards (NIST, ISO) that are applicable to help the Commonwealth meet its governmental requirements.

Our reports are prepared immediately after completing the testing.

Preliminary Drafts

Reporting encompasses both draft and final documents. 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 for it helps them understand *why* each finding is important to the Commonwealth'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 will contain proof of findings in the form of logs, screen shots, IP addresses, and any other proof that the consultants can gather 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:

- Methodology employed
- Positive security aspects identified
- Description of each risk
- Suggested recommendation(s)
- Supporting detailed exhibits for vulnerabilities when appropriate
- Detailed technical vulnerability findings (the specific security concern)
- Detailed technical remediation steps
- Priority of the risk

- Ranked cost or effort
- Supporting detailed exhibits for vulnerabilities when appropriate

Once the Commonwealth has had a chance to review the draft report JANUS will produce the final report.

Final Reports

The final reports are prepared shortly after receiving comments on the draft reports.

JANUS provides additional value to the Commonwealth by supplying more pertinent information than is typical. Each finding is explained in detail and contains the following elements:

- Business risk (potential impact to Commonwealth 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)
- Detailed recommendation/remediation

Both ease of remediation and business risk provide added value and will assist the Commonwealth to evaluate how it will utilize its resources to remediate the problems JANUS uncovers.

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 Commonwealth accompanied by high levels of security – or JANUS can specifically deliver them.

In addition, the PowerPoint presentation will be delivered with 10 hard copies.

Executive Presentation

Upon completion of the tasks, JANUS will schedule an on-site presentation for Executive Management of the Executive Report where project results and recommendations can be reviewed.

JANUS Needs from the Commonwealth

JANUS staff carries its own laptops and tools for testing. However, staff may also require UserIDs and access to computers for verifying compliance with appropriate standards.

When arriving on-site for the wireless testing, it will be necessary to have someone meet our staff to ensure that we are recognized as authorized testers. Otherwise, our staff may be stopped by security. This will ensure that the Commonwealth receives the benefit of as much analysis time as the project anticipates and the schedule allows.

PROJECT MANAGEMENT

Penetration testing and security assessments are specialty areas of ours and we staff our tests with experienced people who possess high caliber technical capability, but also business savvy. Our teams include veterans from such well-known companies as Raytheon and IBM, and from the 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 requirements must be considered within the context of, and be appropriate to, the business 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 security team employees practice multi-tasking on a daily basis within the organization, enabling them to transfer that capability to your needs.

These are the general principles that guide us in staffing a project. However, as each request arrives there are a variety of more specific questions that must be asked. First, what is the network environment? From this initial determination of the application or platform environment we then select staff with the appropriate skills. Is someone who is excellent in web applications and JAVA needed? Is a Red-Hat Linux tester required? After reviewing all the needs of the client, we determine who is available, and when, to calculate who will be able to conduct the testing. From that, a selection of staff proceeds and resumes are selected.

In all situations, we work to pair excellent testers 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 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, QSA, 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. JANUS employees are bonded and undergo background checks (criminal and credit) prior to employment. JANUS also carries Errors and Omissions insurance as an additional level of protection for clients. Employees sign a five-page ethics statement upon entry to JANUS that defines their behavior and stresses that they are to put the needs of JANUS' clients first in all situations.

Project management begins with contact between the Project Manager (PM) and the equivalent at the Commonwealth. From this initial, introductory meeting, you will gain a solid background in how we believe the process should unfold.

Portal capability through SharePoint 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 Commonwealth's information is maintained and provides an easy way for Commonwealth staff to quickly and securely receive results.

Periodic status meetings as indicated in the requirements understanding section 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.

Quality

Quality is also part of JANUS' project management. As consultants to large organizations with complex needs, JANUS subscribes to the standards of true quality and keeps them foremost in its 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 Commonwealth 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.

CONTRACTOR PRIOR EXPERIENCE

In the chart "below", detail three (3) projects your company performed that are similar in nature and scope to the requirements stated in the SOW. Include reference company name and address, contact person with phone number, email address and best time to call, project name, project start and end dates and a brief description of the project.

	Organization Name and Address	Contact Information	Project Title	Project Start and End Dates	Brief Description of the Project*
1	Commonwealth of Massachusetts Information Technology Division One Ashburton Place, Room 811 Boston, MA 02108	Kevin Burns Chief Information Security Officer Phone: 617-619-5696 kevin.burns@state.ma.us Best time to call: Monday – Friday between 9:00 a.m. and 4:00 p.m. EDT	Network and Security Assessment Services	March 5, 2013 – December 30, 2013	JANUS completed a comprehensive analysis of the Commonwealth's IT Network and Security environment and provided a Current-State, Future-State, cost analysis, gap analysis, and road map for moving to the Future-State.
2	Centers for Medicare & Medicaid Services 7500 Security Boulevard Baltimore, MD 21244	Maria McMahon Lead IT Specialist (INFOSEC) (retired) [redacted] – Friday between 10:00 a.m. and 3:00 p.m. EDT	Security Policies and Procedures; Vulnerability/Risk Assessment; Penetration Testing; and System Test & Evaluation (ST&E) Services	September 2001 – August 2013	JANUS has held over a half dozen contracts with CMS over the past 12 years. These projects included an assessment of the entire Agency information security program, review and enhancement of Security Policies and Procedures, and delivery and performance of Vulnerability/Risk Assessment, Penetration Testing, and

					Security Assessment services.
3	Wyoming Department of Health 401 Hathaway Building, 4th Floor Cheyenne, WY 82002	De Anna Greene, CIPP/G, CIPP/IT WDH Compliance Officer Phone: 307-777-8664 deanna.greene@wyo.gov Best time to call: Monday – Friday between 12:00 p.m. and 6:00 p.m. EDT	Penetration and Security Testing	April 2012 – June 2012	JANUS conducted multiple security and penetration tests for WDH. Another task was to perform a PCI DSS Gap Analysis.

*Please see Past Performance Examples for more detail.

JANUS Experience

JANUS is an independent, privately-owned information security specialty consulting company and is the longest operating cyber security company in America. Although we are certified by a variety of state and local government bodies as a woman-owned, small business JANUS has remained in business for over 25 years due to the excellence of its offerings, its dedication to its clients, and its vendor neutral results. JANUS focuses on information security, business resilience, and associated services as its core business and possesses all the depth and experience required to fulfill the Commonwealth's requirements for this project.

As an independent organization that focuses on risk and mitigation JANUS has a natural affinity to protect our clients and bring improvements to their business processes that are all designed to help our clients achieve excellence. JANUS understands that helping the Commonwealth 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 believe our values and complimentary skill sets will exceed the Commonwealth's expectations for this security assessment.

Since JANUS is not affiliated with any hardware or software providers, the Commonwealth can be assured that we have no relationships which would influence our recommendations. The JANUS approach has been well honed by many similar assessments completed each year, and JANUS' staff is experienced and technologically current since they are constantly performing similar tasks for a wide variety of public and private sector clients. Because information security is our specialty, our broad experience and deep expertise allow JANUS to complete more focused analysis at a greater depth than other consulting organizations. The result is that the Commonwealth will receive greater value for its expenditure, in turn, providing greater value to your customers.

A cornerstone of a JANUS assessment is its explanation of business risks related to any technical findings. Every JANUS finding carries with it a delineation of the actual risk to the 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.

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

Company Overview

JANUS has provided security risk/vulnerability assessments and gap analyses for a variety of large, critical institutions including federal, state, and commercial organizations. Federal agencies include the Federal Deposit Insurance Company (where JANUS established the risk management process), the Federal Reserve System Board of Governors, Department of Veterans Affairs (VA), the Federal Trade Commission (FTC), Social Security Administration (SSA), Department of the Interior (DOI), House of Representatives (HoR), as well as the Centers for Medicare & Medicaid Services (CMS) and all of their CMS' Medicare provider contractors where JANUS conducts risk assessments and vulnerability analyses/penetration testing.

JANUS has also completed similar projects for a variety of states including New York, Maryland, Virginia, Massachusetts, North/South Carolina, Wyoming, Wisconsin, and Washington as well as many commercial enterprises throughout the U.S. It is this expertise that has led a number of large critical infrastructure organizations to seek out JANUS for assessments.

In fact, JANUS has held a contract to perform both external and internal security assessments and penetration tests for twelve years at CMS and its insurance partners. JANUS' long commitment to information security and business continuity has provided its consultants with a high level of understanding of the issues that confront complex organizations. This knowledge has been essential in establishing JANUS' standing in this field. JANUS consultants have been described by clients such as Charles Schwab as world-class and are often called upon to speak publicly (in fact our Chief Information Officer just returned from an invitation to speak at an international conference held in Orlando, Florida). Our staff brings an impressive body of experience, a rigorous level of focus on excellence and proven ability to provide client-centric solutions to their assigned projects and regularly receives client ratings of "Excellent". A sample of several of our customer comments is included in this proposal.

Because of its experience and commitment to excellence, JANUS is regarded by clients and peers alike as experts in all activities surrounding the areas of security and continuity. 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 security needs of the organization. JANUS consultants believe in the importance of knowledge transfer with clients, enhancing the lasting impact of its involvement.

A sample group of JANUS' security consulting clients has included such blue-chip organizations as:

- Microsoft
- IBM
- NASA
- Charles Schwab
- Citibank

State government organizations such as:

- New York State

- Commonwealth of Massachusetts
- State of Delaware
- State of Maryland
- State of Texas
- Commonwealth of Virginia
- State of South Carolina
- State of North Carolina
- State of Wyoming
- Washington State

Banking clients such as:

- ABN Amro
- Credit Lyonnais
- UniBanco
- USBancorp
- Valley National Bank
- Fulton Financial

Insurance clients such as:

- Aetna
- The Hartford
- AXA
- Travelers
- Several BCBS organizations

Federal government clients such as:

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

Utilities such as:

- Santee Cooper Power Company of South Carolina
- Occidental Petroleum
- Pacific Gas and Electric
- New York Power Authority

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.)

Higher education clients such as:

- California State University at Sacramento
- University of Texas

- University of Wisconsin
- University of California at Berkeley
- The McCormack Institute of the University of Massachusetts

The breadth of JANUS' technical security work encompasses all major operating platforms: all Windows environments, UNIX, Linux, Novell, and IBM's OS/390 – z/OS as well as many proprietary operating systems; e.g., GE and Honeywell.

A Scan is Not a Penetration Test

For testing projects, JANUS focuses on much more than just scanning. That is only the beginning in our testing. Many organizations sell scanning as a penetration test but it is not. It is only the beginning *part* of a penetration test. JANUS always follows on to provide a full test scenario. A great deal of additional analysis takes place after the scans are complete. Clients have repeatedly stated that our reviews provide more valuable and more specific information about the way they have implemented their security structures versus the way other organizations have supplied similar data. Both the perceived and actual value of the consulting engagement is increased. However, pricing for a scan versus a penetration test is not the same. If the Commonwealth wishes us to scale this down from a full external set of penetration tests please let us know and we will be happy to do so but we have interpreted your request as one requiring full knowledge of the vulnerabilities and exposure identified as well as which are false positives.

False positives left behind by many consulting firms cause organizations a great deal of work after the consulting firm has left. The JANUS methodology investigates each false positive, thus eliminating the work with which the Commonwealth would be left at the conclusion of the project. However, again, there is more time needed to accomplish this, thus pricing is affected. Again, we can adjust downward if the Commonwealth wishes but we have included this work in the proposal.

Another benefit of our assessment is the high quality level of the results, including JANUS reports. 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 your ability to more effectively and efficiently utilize your resources to protect your data, thus to achieve a high return on investment for your expenditure.

Capabilities

Founded in 1988 by Patricia A. P. Fisher, JANUS is America's longest operating information security firm. JANUS specializes in protecting its clients' data and computing environments through:

- Security and risk assessments,
- Infrastructure security testing,
- Information security support,
- Assurance and certification,
- Gap analyses,
- Quality assurance,
- Independent Verification and Validation,
- Data forensics,

- Compliance needs, and
- Business continuity.

JANUS also utilizes all the above skills in assisting its clients transform their IT governance environments to meet future needs through IT Current-State/Future-State assessments, costing, benchmarking, and roadmap development.

We continue to serve a wide range of clients in government and industry and bring the best practices of both sectors to its projects. JANUS is a privately held, certified woman-owned, small business headquartered in Stamford, CT with locations in Boston, MA; Hartford, CT; Austin, TX; and Baltimore, MD.

JANUS’ long commitment to improving infrastructure, IT security, data, and compliance has resulted in its consultants having a high level of understanding of the issues that confront organizations of all sizes. This knowledge has been vital in the establishment of JANUS’ standing in the field. JANUS brings a rigorous focus on excellence and 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 extensive experience within a broad spectrum of settings provides clients with an objective, balanced perspective. JANUS also assists its clients in achieving a proper balance between technology needs and cost.

Having completed many projects that require security management, remediation, and 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-beneficial conclusion for clients.

Service Offerings

JANUS does business throughout the U.S. and globally and has provided services to industry; federal, state, and local government; not-for-profit organizations; and higher education institutions and is eminently qualified and well-positioned to satisfy the Commonwealth’s assessment requirements.

JANUS confronts complex security issues with a clear understanding and appreciation for the operational business objectives of the organization, and helps align and balance those objectives with effective business processes. Further, not only do JANUS consultants possess the technical expertise required, they also believe in the importance of, and achieve whenever possible, knowledge transfer with clients, 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 a completely independent entity, JANUS is not limited by product offerings and is free to identify the best solutions for specific needs, rather than force-fitting specific vendor offerings.

Enterprise-Wide Systems

In early 1989, JANUS took on its 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 database design and implementation, application design, strategy development and business process re-engineering with a strong security orientation.

Significant business followed with firms like GTE Directories in Texas and Florida (now Verizon); where JANUS conducted major business impact analyses advising staff how to improve security processes. Additional assignments included assistance with security administration capabilities in locating, documenting, and categorizing the write-off of out-dated, lost and/or stolen hardware/software. Southern New England Telephone (now AT&T) had JANUS assess its physical and logical capabilities, to determine weaknesses and to perform penetration testing and information security tasks.

Security Management

JANUS' breadth of experience in the security marketplace makes it the ideal candidate for security management assignments. JANUS staff understands the issues confronting our clients' 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 its established reputation for ethics, credentialed experts, and its 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 its work on electronic discovery and breach response/prevention services to form a separate computer forensics practice.

E-Commerce

As Internet usage increased in both business and industry, JANUS responded to clients' e-commerce needs. Adding people to its 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 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; de-militarized zone design, and wireless strategy and design services. The skills gained in providing these services directly impact the capabilities to provide leading edge technical assessment solutions.

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

JANUS' clients are as diverse as the Social Security Administration, The Brookings Institution, BlackRock Financial, Santee Cooper Power Company, Valley National Bank, and Save the Children.

Contractor Personnel and Qualifications

Provide resumes with names of individuals that show the qualifications and skills required to successfully develop and implement the project as defined in the SOW. It is very important that the proposed individuals meet the minimum levels of experience and have all proper certifications, if requested. The proposed project manager must have demonstrated project management skills and technical background and experience to appropriately manage the project. Ensure resumes contain no personal information as these may become public documents.

Project Responsibility

Project manager responsibility for this project will be held by Karl Muenzinger, who has managed many similar projects for a wide variety of government organizations over the past 7 years for JANUS.

Karl Muenzinger is a Project Manager with broad technical experience and best practices in information security and business recovery. With over eleven years experience in Information Security and over fifteen years experience in Information Systems, Mr. Muenzinger's consulting emphasizes information risk management, access controls and identity management, business continuity and disaster recovery planning. He has conducted security assessments 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), and MBCI (business recovery) certifications.

Foad Ardalan is a Certified Information Systems Security Professional (CISSP) with extensive experience in the design, engineering, implementation and support of IT and information security systems. He is experienced in all phases of IT Risk Management and IT Security Audit and testing for identifying and reducing risk, from inside and outside, to the organization. Core competencies include:

- IT risk assessment and security compliance
- Vulnerability management and penetration testing
- Security audit & regulatory compliance
- Access control design and implementation
- Conducting security training and workshops
- Endpoint security design and implementation

Mr. Ardalan is a Certified Ethical Hacker and is a Certified Security Analyst and holds a B.A. in Mathematics and a Masters degree in Telecommunications and Networking.

Mr. Ardalan will lead the technical penetration testing.

Carmen Baughn is a Certified Information Systems Security Professional (CISSP) with extensive experience with penetration testing, vulnerability assessment, and security architecture consulting for multi-tier, internal, external, single and multi-enterprise applications for financial, health-related, and retail services. She also has extensive experience in analyzing policies, procedures, and security practices. She has provided assessments for a wide variety of complex organizations and has provided subject matter expertise to organizations regarding encryption, Payment Card Industry Data Security Standard and Multi-Factor Authentication assessments and implementations including coordination with third party private and federal audit resources. She holds a B.S. in Electrical Engineering.

George Bormes has more than 18 years experience with extensive and diverse technical capabilities in the IT and security environment, emphasizing penetration testing, security network administration and technology assessment. He has performed a wide variety of IT infrastructure and security tests and compliance engineering assignments and is well-versed in operating platforms and system management controls. He has conducted large-organization risk assessments for both government and industry organizations and regularly focuses on client security assessments wherever they might be needed throughout the globe. He is certified by ISACA in the Control of Risk (CRISC).

Daniel Reed has worked as both a software developer (ASP, .NET, java) and as a penetration tester specializing in web applications for JANUS for ten years, where he has worked extensively with web technologies. He has performed security and vulnerability reviews of client websites. He has implemented an authentication framework in a client's training website. He actively assists clients with website development, security evaluations, and environment troubleshooting but his real love is in determining the security problems within web applications.

Note: Please see resumes on next pages.

Resumes

Name	**Karl Muenzinger**		
Position	Project Manager	Clearance	Public Trust Level 6

Experience and Expertise Summary

Mr. Muenzinger provides strategic business perspective in information governance, structure, risk management and compliance for clients in government, finance, and healthcare. With over 33 years of broad technical experience, which includes over 20 years in leadership roles in information security, Mr. Muenzinger offers practical insight and real-world experience in how large, complex organizations manage and respond to Governance, Risk Management, and Compliance issues. Mr. Muenzinger keeps the focus on business requirements, while providing quality-oriented results and best practices in project management. He has a strong understanding of and has worked extensively using banking and NIST security standards.

Education Background

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

Certifications

Certified Information Systems Security Professional (CISSP) – 2001
Certified Information Security Manager (CISM) – 2004
Certified Information Systems Auditor (CISA) – 2009
Member Business Continuity Institute (MBCI) – 2008

Years of Applicable Experience	33 years	Citizenship	U.S. Citizen

History of Applicable Employment Experience

JANUS Associates, Inc. **February 2007 – Present**

Project Manager and Senior Security Consultant

- Project manager for the Financial Industry Shared Assessments Program 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 iSeries security practice. Developed methodology and conducted multiple iSeries risk assessments for a consortium of top-tier financial institutions.
- Produced Risk Assessment and 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.
- Conducted risk assessment analysis for several large, complex federal and private organizations.
- Provides project leadership for information security projects for major clients.
- Managed and produced content for information security training program for federal healthcare agency.
- Performed FISMA security assessments for the Centers for Medicare and Medicaid Services (CMS), in compliance with standards from HIPAA, NIST 800-53, and internal CMS regulations.
- Project Manager for Security Risk Assessments and Accreditation for applications and systems of the City of New York, implemented across a large, multi-campus environment linked using Service Oriented Architecture (SOA).
- Developed and presented executive training: “How to Structure a Good Information Security Program With-Out Breaking the Bank” to the Maryland Education Enterprise Consortium (MEEC).
- Developed and presented executive training: “Compliance Strategy: A Practical Approach to Vendor Assessment” to the International Association of Outsourcing Professionals (IAOP).
- Developed role-based training on electronic records management for a large municipal government.
- Developed and presented webinars on the security aspects of HIPAA Compliance, and on tools for Governance, Risk Management and Compliance (GRC)
- Conducted Security Review and Accreditation of the Business Express application for the City of New York.

Name	Karl Muenzinger

- Project Manager of risk assessment team reviewing the core distributed infrastructure and SCADA systems of a power utility in the northeast and assessed security policies and procedures for a second power utility in South Carolina, based on standards published by the National Energy Regulatory Commission (NERC).
- 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.
- Comprehensive risk assessment and HIPAA Security compliance review of state Medicaid agency, involving over 70 systems and applications that processed Protected Health Information (PHI), and related security policies and business processes. In support of the security review, a comprehensive data classification and Privacy Impact Assessment (PIA) was conducted, including an inventory and diagrammed mapping of the flow of PHI through the organization. The risk assessment also included inspection of security controls of third party Business Associates.

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.
- Motivated and mentored team members on respective areas of expertise, successfully establishing development and operations teams that are fully integrated into the client's application development and change management systems.

UFJ Bank (The Tokai Bank, Ltd.) **1991 – 2002**

Vice President, Information Security Officer

- Initiated the position of Vice President of Information Security. After growing through several technical positions of progressively greater responsibility, Mr. Muenzinger 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, Graham 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 (OCC, FFIEC regulations)
- Information Security project manager for business continuity planning, 50+ disaster recovery drills, information

Name	Karl Muenzinger

security policy development, risk/threat assessment, incident response, firewall management, web filtering and monitoring, antivirus.

System Engineer

- System integration and support for LAN, CHIPS, ACH, SWIFT, FEDLINE, CMS, and trade reconciliation systems.

Den Norske Bank **1989 – 1991**

Lead Programmer Analyst

- Business analysis and system design, AS400 CL, RPGIV.

First Automation Services **1988 – 1989**

Manager, Information Systems

- Managed staff of 15.

Evans & Company **1980 – 1988**

Manager, Information Systems

- Managed staff of ten.

History of Other Experience and Professional Accomplishments

Presented Webinars on the security aspects of Outsourcing, Vendor Risk Assessment, HIPAA Compliance, and on tools for Governance, Risk Management and Compliance (GRC)

Name	**Foad Ardalan**		
Position	Senior Specialist	**Clearance**	Public Trust Level 6

Experience and Expertise Summary

Mr. Ardalan is a Certified Information Systems Security Professional with extensive experience in the testing, design, engineering, implementation and support of information security systems. He is experienced in all phases of IT Risk Management and IT Security Audit and assessment to identify and reduce risk, from inside and outside, to the organization. He is proficient in defining processes for maintaining on-going compliance. Mr. Ardalan has experience with managing global IT projects from initiation and preparation to coordination, negotiation, implementation and rollout.

Education Background

M.S., Telecommunications and Networking - Iona College, New Rochelle, NY – 1997
B.S., Mathematics, Statistics & Computing - Thames Polytechnics, London – 1975

Technical Training/Skills

CISSP (Certified Information Systems Security Professional) – 2005
CEH (Certified Ethical Hacker) – 2011
CSA (Certified Security Analyst) – 2011

Years of Applicable Experience	22 years	**Citizenship**	U.S. Citizen

History of Employment Experience

JANUS Associates, Inc. **February 2012 – Present**

Senior Security Specialist

- Developed training program for Massachusetts State agency for over 4,000 staff (both classroom and content for Computer-Based Training).
- Developed policies and procedures for Massachusetts State agency.
- Performed multiple information security vulnerability assessments for federal government applications for U.S. Centers for Medicare and Medicaid (CMS) focusing on both process and technical environments. He also utilizes, when needed, tools such as HP WebInspect, Nessus, IBM AppScan, Metasploit, and others.
- Developed policies and procedures for European national government finance agency.
- Performed security assessment and advised on remediation activities and processes for national financial organization.
- Developed information security structure and completed multiple policies, standards, and procedures for state-wide critical infrastructure organization.
- Developed and taught compliance and information security risk concepts to statewide financial staff.

Self-Employed **July 2011 – February 2012**

IT Consultant

- Broadridge – Conducted IT Security Audit, including design of RCMs, defining methodology, performing data collection, analysis and reporting on a global IT environment.
- Booz Allen Hamilton (commercial) – Development of methodologies for IT risk management, vulnerability assessment, and penetration testing.

UBS AG, Stamford, CT **March 2001 – July 2011**

Director, IT

Enterprise System Management* *(September 2007 – July 2011)

- Responsible for risk management and product management functions for enterprise-wide products and services.
- Assessed and analyzed the risk to global applications and services on a regular basis for maintaining compliance and reducing risk to the organization.

Name	Foad Ardalan

- Provided mitigation measures to the identified risks and oversaw the implementation of these measures.
- Managed global IT services by analyzing and prioritizing stakeholders' requirements, resource allocation, technology updates, and vendor management for implementing enhancements to meet the business needs.
- Managed global IT projects from product evaluation, selection process, negotiation and development, up to implementation and rollout.

Network Security Engineering/Product Management (March 2001 – September 2007)

- Responsible for engineering, design, implementation and management of secure remote access, end-point security using HP WebInspect, access control and organization-wide data encryption solutions.
- Led the security engineering team responsible for engineering of security products on the global network.
- Participated actively in the design and architecture of the perimeter security concept for the organization.
- Designed and implemented global "remote access", "third party access", and "branch office" connectivity based on Nortel VPN technology.
- Designed and implemented an access management system with two-factor authentication, user provisioning and supporting operational processes, based on RSA SecurID and Cisco ACS.
- Evaluated, selected and globally implemented an "end-point security" solution to meet the security requirements of the organization, based on IBM internet security systems.
- Conducted vulnerability assessments in conjunction with patch management planning.
- Managed the end-to-end global implementation of the Citrix project.
- Achieved SOX compliance though assessment and implementation of risk mitigation measures.

Perot Systems, Stamford, CT **1998 – 2001**

Associate

Network Security Engineering

- Responsible for the engineering and support of network security systems.
- Implemented, supported and monitored Checkpoint firewalls on the global network.
- Implemented different encryption methods for securing data communications over the public and private communication links through the use of VPNs, Cylink, and implementing certificates.
- Assisted in the development and implementation of security policies and awareness programs.

Union Bank of Switzerland (UBS) **September 1990 – July 1998**

AVP

Global Network Monitoring Engineer (January 1995 – July 1998)

- Responsible for implementation and integration of systems and network management products.
- Designed, engineered and implemented the "Technology Monitoring Center" consisting of several element managers with integration into the event management system, reporting and trouble ticketing systems. The implementation helped the organization to detect issues proactively, increase availability and reduce down time to business services.

System Administration & Support (September 1990 – January 1995)

- Responsible for system administration activities on distributed systems.
- Managed system administration and day-to-day operational activities on a network of UNIX servers.

NCR & HP Dealerships, Dubai **1985 – 1990**

Pre-Post Sales Engineering

Sales Support Engineer

- Responsible for technical pre-sales discussions and post-sales customer support activities in NCR and Hewlett-Packard local dealerships.
- Held pre-sales technical discussions with potential customers.
- Provided post-sales customer support.
- Assisted & trained customers on patch management, release introductions, and demonstrated new features & functionality of the products as they became available.

Name	**Foad Ardalan**

Other Activities

Norwalk Community College, Norwalk, CT **2006 – Present**

Adjunct Professor

Teaches evening courses in “Security Management Practices” and “Security Operations” covering Security Policies; Standards & Guidelines; Risk Management Workshops; Security Architecture; Access Control Implementation; Workshops on regulatory requirements, e.g. PCI DSS, Network Security, Cryptography, Logging & Monitoring

Name	**Carmen Baughn**		
Position	Senior Consultant	**Clearance**	Public Trust Level 6

Experience and Expertise Summary

Ms. Baughn is a Certified Information Systems Security Professional (CISSP). She has extensive experience with security risk assessments and architecture consulting for multi-tier, internal, external, single and multi-enterprise as well as analyzing policies, procedures, and security practices. She has provided assessments for a variety of complex organizations and has successfully led password synchronization and firewall analyses and upgrades, and provided subject matter expertise for encryption, Payment Card Industry Data Security Standard and Multi-Factor Authentication implementations including coordination with third party private and federal audit resources. Ms. Baughn has extensive experience with Project Management, Quality Assurance, Problem and Change Management Methodology. She has led change and problem management activities, including change management boards, morning problem reviews and new application assessments, for web enabled, client/server and legacy applications. She has updated Systems Assurance procedures and performed one-on-one training for tools and procedures as well as produced management reports on a daily, weekly and monthly basis.

Education Background

Bachelor of Electrical Engineering, Auburn University, September 1979 – March 1984 (Graduated)

Post Baccalaureate study in Ethics, University of North Florida, September 2009 – September 2010

Certifications and Technical Training/Skills

Certified Information Systems Security Professional (CISSP) – March 2010

Skills: Security Architecture - CA SiteMinder, Active Directory, RACF, Sun Directory Server, IBM TAM and WebSphere; Operating Systems - (Client/Server and Distributed) - Windows, Linux, OS/2, UNIX, MVS; Languages - C, C++, SQL, Ada, Pascal, Fortran, Basic and Assembler; Design Methodologies - Object Oriented, Relational Modeling and Structured Analysis; Tools: Project Server, SharePoint, Office, DB2, Platinum.

Training: Total Project Management (company customized method based on PMBOK), RSA 2007 Conference, MISTI Information Security Conference 2003, Project Management 1, Advanced SQL, C Language Training, Object Oriented Analysis and Design, Structured Analysis and Design, Total Quality Management leader training.

Years of Applicable Experience	23 years	**Citizenship**	U.S. Citizen

History of Employment Experience

JANUS Associates, Inc. **July 2011 – Present**

Senior Security Consultant

- Led major risk assessment and implementation program for improved information security processes for Republic of Georgia Ministry of Finance.
- Performed risk assessment for State of Washington.
- Lead analyst for assessment of State IT environment to develop future direction and roadmap for implementation.
- Completed multiple risk assessments for U.S. Centers for Medicare & Medicaid.
- Performed risk assessment for smart-grid design project.
- Completed analysis of security policies and procedures for state Agency.
- Performed security analysis for major corporate mainframe environment.
- Completed multiple security vulnerability assessments for federal health care agency.

Consulting Spectrum, Inc. at Winn Dixie Corporate **2009**

Security Manager Consultant

- Managed security group under a four month contract to provide seamless leadership while the permanent Security Manger was on leave.

Name	Carmen Baughn

- Achievements: Payment Card Industry (PCI) audit and certification.
- Responsibilities: Security architecture consulting - retail customer kiosks, People Soft resource recruiting, store inventory management and data center solutions. Operations - Managed security administration team of five analysts for hires, moves, terminations, file and system access, SOX reporting, web-usage monitoring, legal support and management escalations.

Fidelity Information Services/Lender Processing Services **1994 – 2008**

Security Architect/IT Specialist

2003 – 2008 - Systems Security Project Office

- Managed and was a working member of the security architecture team responsible for security of application and data center infrastructure development and updates.
- Achievements: Led the 2006 and 2007, NIST 800-30 based IT enterprise risk assessment and security strategy planning. Developed solutions for Payment Card Industry (PCI), encryption, multi-factor authentication and web based applications. Managed projects for firewall, SiteMinder, Directory Server, Blockade password synchronization, multi-factor authentication and security awareness training. Speaker at two sessions of the 1997 Mercury Interactive (HP) Users Conference in Orlando.
- Responsibilities: Security architecture consulting for the Lending Portal and suite of 12 hosted mortgage lending applications as well as legacy mainframe applications on secure coding practices, access control design, test data management, application ID's, multi-factor authentication, architecting for separation of duties, testing and implementing on hardened operating systems and building applications compatible with secure data bases and separation of networks. Developed QA test scenarios for secure coding and validating web application security components. On-call user administration for RACF including JCL runs from TSO to create and reset user ID's.

2000 – 2003 International Project - United Kingdom Testing Liaison

- Managed the test environment and application development relationships including defect documentation and resolution planning. Administered operations and QA application access for ID's in Active Directory, Sun UNIX, application specific on the web tier and mainframe.

1999 – 2000 Systems Assurance

- Audited change and problem management processes for web enabled, client/server and mainframe applications.

1994 – 1999 Software Test

- Lab setup, script generation, test plans, requirements analysis, data validation, report generation and User Interface standards conformance. Performance test of client/server and web applications with HP WinRunner and LoadRunner.
- Tool selection, on-going lab maintenance, tool training, script generation, data validation, and problem reporting for multiple Mortgage Lending Products.
- Design Lead (five designers) - Led Business Object Analysis of data stored in legacy VSAM files.

Lockheed Design Integration Group **February 1993 – February 1994**

Scientific Programmer

- Software Test Lead – under LYNX (real time UNIX) supervised one software designer.

TRW Systems Integration Group **November 1989 – February 1993**

Member of Technical Staff

- Software Developer responsible for detailed design, unit code, unit test and process integration planning. The product runs in a distributed environment. Host and client run on Silicon Graphics UNIX operating systems.
- Manager and Technical Lead supervising three software designers.

Harris Corporation **May 1984 – November 1989**

Senior Engineer

- Work Package Leader supervising three engineers to write simulation models on Computer Aided Engineering tool (in PASCAL). Performed manufacture analysis of a classified digital module. Designed digital synthesizer.

Name	**George Bormes**		
Position	Technical Testing	**Clearance**	Public Trust Level 6

Experience and Expertise Summary

Mr. Bormes has more than 18 years experience with extensive and diverse technical experience in the IT field, emphasizing security and network administration and technology assessment. He has performed IT infrastructure and security administration and engineering assignments. He is versed in operating platforms, system management controls, and Cisco troubleshooting, and has conducted large-organization risk assessments for federal agencies.

Education Background

B.S., Business Administration, University of Wisconsin, 1987

Certifications and Technical Training/Skills

Certified in Risk and Information Systems Control (CRISC) – 2011

Metasploit Framework, WebScarab, Nessus, Cin and Abel, Nikto/Paros, MS-DOS, all Windows desktops and servers (operating systems), Antivirus products, Lotus Domino 4, 5 and 6, Microsoft Outlook, Microsoft Exchange Server, Remotely Anywhere, VNC, Sniffer Pro, MS Office, MS Outlook, Lotus SmartSuite, Norton, PC Anywhere, multiple scanning and vulnerability tools.

Third-Party Lotus Notes Training V3-6, 1994 – 1999

Years of Applicable Experience	18 years	**Citizenship**	U.S. Citizen

History of Applicable Employment Experience

JANUS Associates, Inc. **March 2005 – Present**

Sr. Engineer II

- Performed security control assessments for large federal healthcare agency for over 7 years.
- Performed security testing for HIPAA requirements for federal agencies and their contractors.
- Conducted FISMA assessments for federal agencies.
- Completed external and internal application testing for large number of government, commercial, not-for-profit clients.
- Performed network scans (both internal and external) and internal network testing for large variety of clients.
- Performed risk assessments of distributed systems for Veterans' Affairs, the Centers for Medicare and Medicaid Services (CMS) and the Federal Trade Commission.
- Completed Certification and Accreditation (C&A) assessments for CMS, New York City, private industry, and federal contractors.
- Performed Black Box application security assessments. Conducted web application testing for various client companies, both nonprofit (government) and for-profit entities. Findings were noted, explained and written up in a formal report to be presented to management. Reports included information on the business risk to the organization, a high-level analysis of the issues discovered, as well as recommendations for mitigation where possible or appropriate.
- Performed security audits for CMS and its contractors – both policies and procedures audits and technical testing of distributed systems.
- Completed security audit support assistance for federal contractors to ensure required controls exist.
- Participated in writing a Disaster Recovery plan for a non-profit organization with the need for a highly resilient system.

Scalabit Solutions LLC **April 2003 – March 2005**

IT Consultant/Network Architect

- Launched Scalabit Solutions, an IT consulting firm dedicated to designing and implementing cost-effective technical solutions for small to medium-sized businesses. Services include network design & installation,

Name	George Bormes

systems analysis & upgrades, security backups, and troubleshooting.

- Designed and implemented network for e-commerce consulting startup for Requisite Design LLC.
- Installed and configured Cisco routers for internal networks
- Installed and configured Cisco switches to allow for VLANs.
- Designed and implemented network for large, global vendor of duty-free merchandise sold through several airlines (Inflight Sales Group (ISG)).

Provided network support for specialty metal fabricator for Sigmund Cohn Corp.

Mentor Communications Group **1998 – 2003**

IT Systems Manager

- Planned, managed, and optimized the operation of multi-domain Lotus Domino educational software company specializing in multimedia solutions.
- Redesigned and reworked network infrastructure to permit more efficient management.
- Responsible for all troubleshooting of Cisco routers and switches on a day-to-day basis.
- Established and implemented all Lotus Notes-related functions and top level systems considerations such as data security and disaster recovery.
- Detailed and implemented security policies and procedures to be used by the Systems Group. These policies and procedures were the first formal articulation of a systems security mission for the company.
- Supervised IT support staff and acted as the point contact for all systems-related issues.
- Planned, managed and executed company-wide migration from Lotus Notes R4 to R5 with no disruption to daily operations. Defined and implemented test standards to ensure that all upgraded databases maintained security protocols, data integrity, and consistency.
- Significantly improved overall IT performance and stability by establishing new quality assurance standards and reengineering all system hardware and software to meet the diverse requirements of several demanding departments. Company survey reflected high satisfaction ratings for improved functionality and efficiency throughout the entire organization.
- Developed several innovative applications to improve internal business processes and support needs of specific project teams and clients. Implemented new bug reporting and tracking system that significantly reduced IT response time to problems reported by end users.
- Strategically planned, coordinated, and led corporate relocation to larger facility. Defined and established systems structure for new environment. Multi-phased relocation process was successfully completed on time and within the budget with minimal disruption to end users.

Keane Consulting for the National Institute of Standards & Technology (NIST) **1995 – 1998**

Consultant

- Provided IT consulting services to several major clients.
- Responsible for tracking and fixing bugs and implementing enhancements throughout the development of a highly complex Lotus Notes Application. High client satisfaction increased the scope of the engagement to creating several customized applications using Notes formula language and LotusScript.
- Oversaw day-to-day operations of Lotus Notes network for 150 users. Developed a customized Notes application to track jargon usage and provide a discussion forum for the documentation team. Conducted security audit on Notes network and implemented improvements. Configured Domino server to provide Internet access.

Tascor Consulting for IBM **1992 – 1995**

Technician

- Created and staffed a helpdesk serving 3300 users worldwide. Group received high acclaim throughout IBM's Global Consulting Group for significantly improving productivity through modifications that resulted in improved usability and efficiency.
- Supervised daily operation of a global Lotus Notes infrastructure using TCP/IP, WAN and modem connectivity with over 80 servers and 3300 users. Responsibilities included network administration, software configuration,

Name	George Bormes
replication scheduling, troubleshooting, and server deployment of servers, workstations and laptop PCs. • Provided second and third line technical support and training for both mobile and LAN-connected workforce. • Created a highly effective Windows-based software platform to meet the specific needs of a diverse, mobile workforce.	

Name	**Daniel Reed**		
Position	Technical Testing	**Clearance**	U.S. Government High Public Trust Level 6

Experience and Expertise Summary

Mr. Reed is a lead security analyst, penetration tester, and software developer (ASP.NET, Java) with 15 years diverse technical, programming, and information security experience. He is a .NET developer with extensive experience in ensuring the security of applications and infrastructures, specializing in web applications where he has worked extensively with web technologies and in conducting penetration testing for complex systems. He also has performed security and vulnerability reviews of client websites. He has implemented an authentication framework in a client's training website. He actively assists clients with website development, security evaluations, and environment troubleshooting. Mr. Reed has a strong and diverse IT background.

Education Background

University of Pittsburgh at Johnstown; 40 credits toward Major in Computer Science; 1994 – 1996
Community College of Allegheny County; 60 credits toward Major in Computer Science; 1996 – 1997, 1998 –1999

Languages/Other Technical Skills

C, C++, C#, ASP.NET, Visual Basic.NET, WSDL, SQL, Javascript, Java, HTML, XHTML, CSS, PHP, Coldfusion

Created, tested, used, and managed VMWare virtual images for numerous operating systems. Virtual Machines were used to test and debug custom created in-house software applications spanning multiple clients, servers, and domains. Multiple penetration testing tools for customer tests of applications.

Years of Applicable Experience	15 years	**Citizenship**	U.S. Citizen

History of Applicable Employment Experience

JANUS Associates, Inc. **May 2004 – Present**

Staff Security Engineer

- Developed and implemented a Learning Management System for hosted training programs in large, complex operations.
- Performed a comprehensive security review of a cloud-based federal government computing facility leading to facility becoming one of the first US government approved cloud providers.
- Conducted network and application penetration tests and vulnerability analyses for large, complex government and commercial organizations.
- Performed security vulnerability tests for multiple state agencies.
- Performed security code reviews for applications for large client environments.
- Developed a single sign on application to securely connect state government agency with state-wide locations.
- Implemented a secure logon system for federal government Computer Based Training (CBT) application using Windows Authentication.
- Updated logic in CBT to make the site more robust and user friendly for all aspects of training and certification of CMS employees.
- Implemented changes to CBT database which uses Microsoft SQL Server. These changes were needed for additional features added to the CBT site and to increase site performance.
- Updated the method in which the CBT site connects to the SQL Server database, making the database connections more secure and stable.
- Extensive experience with all aspects of security application and identity management software standards and solutions such as BioApi and CDSA frameworks, GINA, server, administrator, MMC administrator.
- Created a Novell authentication method using JANUS' application technology. Created both the client and server portions of the Novell method.
- Created numerous applications, utilities, and testing applications. Examples include a secure biometric Prep Tool which had various functions, such as extending Active Directory and creating biometric settings in Active

Name	Daniel Reed

Directory, and generating a symmetric key. This was completed in C, C++, C#, VB.NET, and WSDL.

- Worked on large portion of application build process. Maintained and updated build and created scripts for installing application debug deliverables and scripts for organizing deliverables so that they can then be easily imported into the installer projects.
- Created installers for all of JANUS' applications using InstallShield. In charge of creating and maintaining the installer.
- Worked on implementing licensing in and generating software application licenses in secure manner.

Fox Learning Systems **May 1999 – May 2004**

Lead Software Developer/Software Engineer

- Managed development team. Coordinated resources from designers, editors, videographers, and healthcare professionals to create marketable products. Independently responsible for both main product lines. Controlled decision-making for software architecture.
- Interviewed, hired, trained, integrated, and organized new employees into productive software development team.
- Lead developer/software engineer of Eldercare Family Center. Developed in HTML, CSS, JavaScript, ColdFusion MX, MySQL, Flash MX, with an Apache web server.
- Significantly reduced materials cost and man-hours by introducing and implementing secure license management system to CD-ROM based software.
- Designed and coded Employee Safety Series, a kiosk-style training program funded in partnership with Royal & SunAlliance. Developed in Visual Basic, Macromedia Authorware, SQL, and Crystal Reports.
- Designed and coded software demonstration of Eldercare Family Center, resulting in government funding to develop full product.
- Redeveloped, recoded, and maintained secure corporate website HTML, JavaScript, CSS, Microsoft Access, and ColdFusion.
- Reengineered company's main product line using Visual Basic Macromedia Authorware, SQL, Microsoft Access, and Crystal Reports.
- Debugged, and re-coded entire Solutions for Long Term Care product line.

Social Security Administration **April 1999**

Network Engineer

- Installed numerous servers and workstations for the Social Security Administration as part of a project team.

Domestic Workforce Utilization

Complete and sign the Domestic Workforce Utilization Form Attachment C.

Attachment C

DOMESTIC WORKFORCE UTILIZATION CERTIFICATION FOR MULTIPLE AWARD CONTRACTS (07/24/09)

To the extent permitted by the laws and treaties of the United States, this certification will be used by the Agency in making a best value selection for each particular assignment. Each quote will be evaluated for its commitment to use the domestic workforce in the fulfillment of the contract. Maximum consideration will be given to those suppliers who will perform the contracted direct labor exclusively within the geographical boundaries of the United States or within the geographical boundaries of a country that is a party to the World Trade Organization Government Procurement Agreement. Those who propose to perform a portion of the direct labor outside of the United States and not within the geographical boundaries of a party to the World Trade Organization Government Procurement Agreement will receive a correspondingly smaller score for this criterion. In order to be eligible for any consideration for this criterion, suppliers must complete and sign the following certification. This certification will be included as a contractual obligation when the contract is executed. Failure to complete and sign this certification will result in no consideration being given to the supplier for this criterion.

I, Patricia Fisher, President & CEO **[title]** of JANUS Software, Inc. (d/b/a JANUS Associates) **[name of Contractor]** a Florida **[place of incorporation]** corporation or other legal entity, ("Contractor") located at 1055 Washington Boulevard, Stamford, CT 06901 **[address]**, having a Social Security or Federal Identification Number of [redacted], do hereby certify and represent to the Commonwealth of Pennsylvania ("Commonwea[redacted]e of the boxes below):

✓ All of the direct labor performed within the scope of services under the contract will be performed exclusively within the geographical boundaries of the United States or one of the following countries that is a party to the World Trade Organization Government Procurement Agreement: Aruba, Austria, Belgium, Bulgaria, Canada, Chinese Taipei, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hong Kong, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Latvia, Liechtenstein, Lithuania, Luxemburg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Singapore, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, and the United Kingdom

OR

_______________ **percent (_____%) [Contractor must specify the percentage]** of the direct labor performed within the scope of services under the contract will be performed within the geographical boundaries of the United States or within the geographical boundaries of one of the countries listed above that is a party to the World Trade Organization Government Procurement Agreement. Please identify the direct labor performed under the contract that will be performed outside the United States and not within the geographical boundaries of a party to the World Trade Organization Government Procurement Agreement and identify the country where the direct labor will be performed:

____

____

[Use additional sheets if necessary]

The Department of General Services **[or other purchasing agency]** shall treat any misstatement as fraudulent concealment of the true facts punishable under Section 4904 of the *Pennsylvania Crimes Code*, Title 18, of Pa. Consolidated Statutes.

Attest or Witness:

[redacted]/11/14
ture/Date

Lyle Liberman, Chief Operating Officer
Printed Name/Title

JANUS Software, Inc.
Corporate or Legal Entity's Name

[redacted] 4/11/14

Patricia A. P. Fisher, President & CEO
Printed Name/Title

Small Diverse Business Participation

To maximize DGS-certified Small Diverse Business participation in the project, the greatest consideration will be given to a Small Diverse Business bidding as a prime contractor. For all other prime contractors subcontracting to a Small Diverse Business, briefly explain what your company's approach will be to maximize Small Diverse Business participation in the project if you are selected for award. This should include detail on which portions of the contract will be performed by the Small Diverse Business. Include specific percentage commitments to be paid to Small Diverse Businesses based upon the total contract value. The more definitive the commitment and the greater the percentage commitment, the greater consideration that your company will receive for this best value selection factor.

JANUS is a certified woman-owned, small business that has been successfully serving government and industry clients for over 25 years in performance of exactly this type of task.

Past Performance Examples

<table>
<tr><td colspan="3"><b>Contract Name: Network and Security Assessment Services</b>
<b>a. Customer Name: Commonwealth of Massachusetts Information Technology Division (ITD)</b></td></tr>
<tr><td><b>b. Contract/Purchase Order Number:</b>
CT-ITD-2013RFQ1320JANUS</td><td><b>c. Contract Type:</b>
FFP</td><td><b>d. Total Contract Value:</b>
$1.29MM</td></tr>
<tr><td colspan="3"><b>e. Brief Description of Work Performed:</b>
JANUS completed a comprehensive analysis of the Commonwealth’s IT Network and Security environment taking into account:
• Current-State Network and Security Services
• Network Security Cost and Analysis Document
• Future-State Network and Security Services Document
• Network Security Services Recommendations Document
The project included completion of a comprehensive information security and network operations analysis of the Commonwealth’s IT structure. From this, a report was prepared that described the Current-State of both elements of focus. Following this, a financial assessment of ITD’s network services and security services was completed with a focus on “business truth” of where ITD is today. In this, JANUS provided a “leading practices” focus to describe where ITD stood in relation to similar organizations.
JANUS then prepared an analysis of where ITD and the Commonwealth might be for a Future-State environment. In this, JANUS focused on all components of the security and networking services operations and developed dashboards describing where ITD was currently, and where it might be over a period of time (covering 5 years).
JANUS also provided a sound business plan strategy that effectively and efficiently moves ITD from the Current-State to the Future-State service along with a detailed roadmap in how to get to the Future-State.
ITD embraced the recommendations and began implementation based on the roadmap JANUS provided before the project was completely finished.</td></tr>
<tr><td><b>f. Period of Performance:</b>
March 5, 2013 – December 30, 2013</td><td><b>g. Technical/Project Manager:</b>
Kevin Burns
Chief Information Security Officer
One Ashburton Place, Room 811
Boston, MA 02108
Phone: 617-619-5696
Fax: 617-626-4411
kevin.burns@state.ma.us</td><td><b>h. Contract Officer:</b>
Annemarie Kates
Phone: 617-626-4437
annemarie.kates@state.ma.us</td></tr>
</table>

a. Customer Name: Centers for Medicare & Medicaid Services (CMS), Department of Health & Human Services (DHHS)

b. Contract/Work Identification Numbers:	**c. Contract Type:**	**d. Total Contract Value:**
CMS 01-01177 CMS 02-0111 HHSM-500-2006-00071G - - - - - - - - - - - - - - - CMS 03-01126 HHSM-500-2005-00014G HHSM-500-2006-00052G	FFP - Task Orders NTE Time & Materials	CMS 01-01177: $883K CMS 02-0111: $4.1MM HHSM-500-2006-00071G: $1.7MM (with options) - - - - - - - - - - - - - - - CMS 03-01126: $4.1MM HHSM-500-2005-00014G: $1.9MM HHSM-500-2006-00052G: $8.4MM

e. Brief Description of Work Performed:

The Centers for Medicare & Medicaid Services (CMS) contracted with JANUS Associates, Inc. for a number of projects to support its information security program and FISMA processes. JANUS has held over a half dozen contracts with CMS over the past 12 years. These projects include assessment of the entire Agency information security program, review and enhancement of Security Policies and Procedures, and delivery and performance of Vulnerability/Risk Assessment, Penetration Testing, and System Test & Evaluation (ST&E) services where a detailed understanding of laws, regulations, and Personally Identifiable Information (PII) requirements were crucial.

The CMS computing environment and infrastructure process and support all Medicare Enrollment and Claims handling functions across the United States with widely varying mainframe environments (including RACF, CA-Top Secret and ACF2) and distributed platforms (Novell, UNIX, Windows). In completion of its many ST&E assignments, JANUS applies knowledge of all the legislative, regulatory, and agency-specific guidelines as well as industry best practices and HIPAA guidance.

CMS' general support systems (GSSs), major applications (MAs), and other applications support over 4,000 employees at CMS' central site in Baltimore, and in 10 regional offices in major cities throughout the country. CMS also has over 60 business partners throughout the US and works with state governments of all 50 states in meeting the needs of approximately one in four Americans and with expenditures to meet its program goals of over $344 billion (20% of the Federal Government's dollars).

CMS' Office of Information Services (OIS) Security Standards Group first engaged JANUS to review the adequacy and effectiveness of the information security program at CMS. JANUS designed an enterprise-wide business process review, developed instruments with which to undertake an analysis, completed over one hundred individual interviews, designed statistical analysis techniques to derive results of the efforts, and prepared a thorough and detailed report oriented towards both management and technical readers. JANUS made strategic recommendations to improve the program and meet future needs. Further, JANUS mapped existing CMS security standards to NIST standards, legislative requirements, and industry best practices. Where this matrix indicated gaps existed in the CMS program, JANUS recommended solutions designed to obviate the risks. As requested by CMS, JANUS then executed these recommendations according to their priorities (which JANUS had worked on with CMS to determine). Three of these – the "Minimum Security Safeguards" standards, the Risk Assessment (RA) Methodology, and the Risk Assessment (RA) Template for completing assessments by business owners – have been acknowledged by NIST as examples of "best practices". In ongoing services, JANUS prepares information security policies, additional guides and user requirements, and supports the information security program, in total.

In a second contract with CMS, JANUS executed a variety of action plans identified in the above to achieve broad-based implementation throughout the larger CMS environment. To this end JANUS prepared 15 information system security plans for systems owners, and worked with them to manage the level of security required to make improvements throughout the system development life cycle where needed.

JANUS was also tasked with moving security standards (and their implementation) as they applied to CMS's IT modernization program out into the business processes so that security is built-in to all new application development endeavors. CMS' IT modernization program is based on a three-tier architecture model that identifies the presentation, application, and data layers that must be separated by firewalls. In order to ensure that new systems comply with that architecture, JANUS reviewed the security implications of all new system design architectural documentation and schematics. JANUS also works with CMS business owners to assist them with the security architecture of their designs. Where needed, JANUS staff makes recommendations for improvements and/or corrections and works with system owners to ensure that the design reflects these architectural additions. JANUS recommends to the Office of Information Security - Security and Standards Group acceptance or rejection of the designs.

In addition to performing assessments across the United States for all Medicare claim handlers JANUS performed similar services for CMS' own computing environment. This infrastructure is a large scale, highly networked, mixed platform environment comprising MVS (i.e., OS/390 and z/OS) mainframes, distributed processing platforms (e.g., MS Windows and UNIX), and TCP/IP network and networking components (e.g., routers and firewalls). The overall environment includes both a CMS agency data center and equipment, and corporate assets providing services to the agency via contracted agreements.

JANUS also designed for CMS a vulnerability tracking and reporting system-allowing 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. Plans of Action take into account milestones, risks to the projects, and possible issues that require additional focus. This approach enables JANUS clients to take an exception-based view of projects, thus saving them time and effort related in their oversight responsibilities.

f. Period of Performance: CMS 01-01177: 09/2001 – 09/2002 CMS 02-0111: 08/2002 – 09/2008 HHSM-500-2006-00071G: 06/2006 – 08/2011 - - - - - - - - - - - - - - - CMS 03-01126: 08/2003 – 08/2007 HHSM-500-2005-00014G: 01/2005 – 09/2006 HHSM-500-2006-00052G: 06/2006 – 06/2007 plus 4 options	g. Technical/Project Manager: Maria McMahon Lead IT Specialist (INFOSEC) (retired) [redacted]	h. Contract Officer: Candice Savoy Contract Specialist Phone: 410-786-7494 FAX: 410-786-9088

Contract Name: Security Review and Assessment
a. Customer Name: Maryland Department of Labor Licensing and Regulation (DLLR)

b. Contract/Work Identification Number: 96120	**c. Contract Type:** FFP	**d. Total Contract Value:** $24,651.00

e. Brief Description of Work Performed:
Internal assessment and external penetration test of all vulnerabilities associated with DLLR systems being exposed to the Internet. JANUS conducted a number of tasks including:

1. Review of existing policies and procedures
2. Review of publicly accessible network devices
3. On-site visit and review of DLLR's Data Centers
4. Vulnerability Assessment report referencing the appropriate standard and other industry best practices.

In addition, JANUS provided external security testing of the environment. In which it sought to gain access to the client network by penetrating, or circumventing, protection mechanisms. To accomplish this, JANUS testing included:

- Internet vulnerability scanning
- Evaluation of IP address range
- Internet firewalls
- E-mail server
- Web Server
- Other devices identified during testing

Vulnerability Assessment
The vulnerability assessment represented an independent third party review of DLLR's Infrastructure with a focus on testing a set of DLLR's infrastructure comprising twenty (20) servers. JANUS reported vulnerabilities to DLLR in a single report with two (2) sections: an executive summary and a detail summary intended to be used by DLLR engineers for remediation. The report focused on compliance, policy and procedure maturity and the security controls protecting data. The detailed reporting referenced specific compliance standards.

f. Period of Performance: November 1, 2012 – December 20, 2012	**g. Technical/Project Manager:** David Stine Chief of Technology Office of Information Technology Maryland Department of Labor, Licensing and Regulation 500 North Calvert Street #401 Baltimore, MD 21202 Phone: 410-767-2889 dstine@dllr.state.md.us	**h. Contract Officer:** N/A

Contract Name: Unemployment Insurance Vulnerability Assessment Project
a. Customer Name: Massachusetts Executive Office of Labor and Workforce Development (EOLWD)

b. Contract/Purchase Order Number: ITS43	**c. Contract Type:** Firm Fixed Price	**d. Total Contract Value:** $210,000.00

e. Brief Description of Work Performed:

JANUS was contracted to perform several risk assessment projects for EOLWD. JANUS assisted EOLWD in preparing materials that EOLWD will submit for FISMA-based certification and accreditation of systems by performing risk assessments, including the following tasks:

- Review/update system boundaries and EOLWD baseline security requirements,
- Conduct/document risk assessments
- Update System Security Plans (facilities, hardware, network, and OS) to reflect the security posture for the new QUEST system, and
- Prepare a Security Test and Evaluation Plan that documents the methodology and technical approach to vulnerability assessment, objectives, and procedures that will be utilized during the risk assessment scanning phase.

JANUS performed a vulnerability assessment of the QUEST Revenue system, consisting of port scans and automated vulnerability scanning, followed by verification and analysis of vulnerabilities found in the scans, followed by attempts to exploit vulnerabilities using “white hat” penetration testing methods.

JANUS completed an on-site assessment of the application security surrounding the QUEST Revenue application and performed a vulnerability assessment of the QUEST Benefit system, following the same methodology as the assessment of the Revenue system.

JANUS completed a security audit of the EOLWD telephony system. The security audit focuses on security configuration, policies and procedures, as well as physical and environmental security of telephony closets.

JANUS performed an additional review of an unemployment application under development utilizing penetration testing and on-site analysis to determine the full extent of possible problems and provide guidance to the department as it completes implementation.

f. Period of Performance: September 2011 – July 2012	**g. Technical/Project Manager:** James O. Newman Information Security Officer Office of Internal Control & Security Executive Office of Labor & Workforce Development Charles F. Hurley Building 19 Staniford Street, 4th Floor Boston, MA 02114 Phone: 617-626-6283 jnewman@detma.org	**h. Contract Officer:** N/A

Contract Name: State of Wyoming Penetration and Security Testing
a. Customer Name: Wyoming Department of Health (WDH)

b. Contract/Purchase Order Number: Multiple projects	**c. Contract Type:** Firm Fixed Price	**d. Total Contract Value:** $15,000.00

e. Brief Description of Work Performed:

JANUS conducted multiple security and penetration tests for the Wyoming Department of Health (WDH). The latest project for testing focused on a single major application for which the State was interested in ascertaining the risks. The objectives of this latest task were:

1) To represent an independent third party review of a major application system installed in the State of Wyoming.
2) To report vulnerabilities to WDH in a single report that includes an executive summary and detailed findings to be used for remediation.
3) To reference requirements of the Payment Card Data Security Standard (PCI DSS) to provide a base for understanding compliance issues.

A second task was to perform a PCI DSS Gap Analysis to enable WDH to understand their potential risks as well as what is needed to achieve compliance.

For the Gap Analysis JANUS performed:

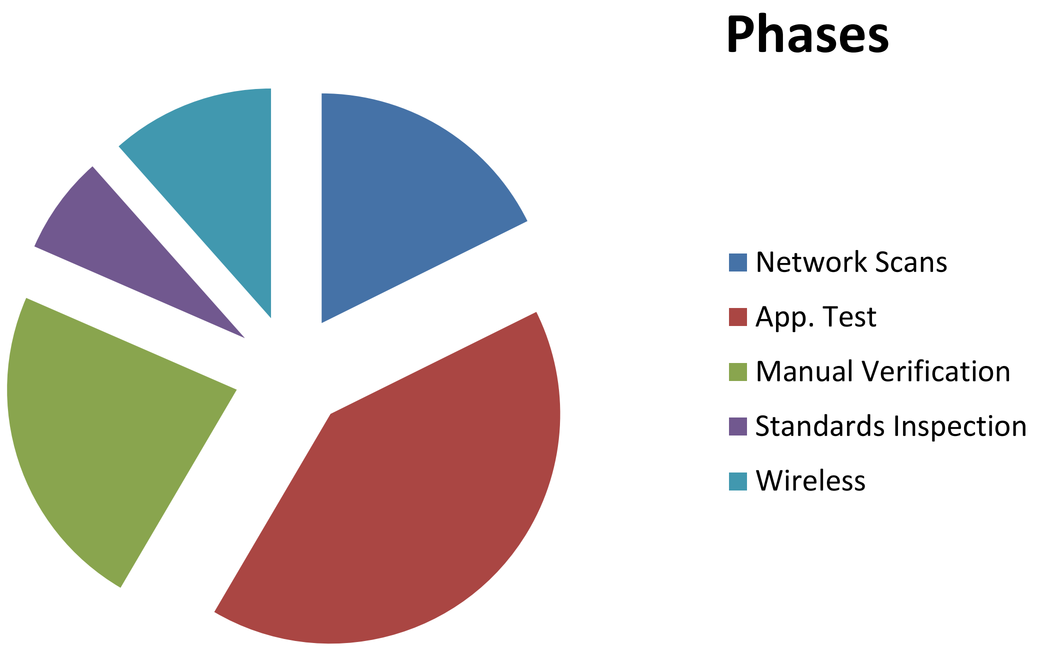
- A review of the application to understand where the State is not in compliance with PCI standards. This gap analysis prepared the State to undergo its PCI audit after it had an opportunity to understand any gaps that existed and to resolve any potential issues. This process assisted the State avoid a more costly audit which usually reveals issues that must be remediated prior to achieving compliance – and then repeating that audit. The Gap Analysis provided the method most organizations are following to bring them to the point where they can pass a compliance audit.

The deliverables for this project were:

- A Penetration Test report sufficient to fulfill section 11 of the PCI DSS, as well as referencing any applicable federal standards or industry best practices.
- One gap analysis focusing on the selected application.

f. Period of Performance: April 2012 – June 2012	**g. Technical/Project Manager:** De Anna Greene, CIPP/G, CIPP/IT WDH Compliance Officer Wyoming Department of Health 401 Hathaway Building, 4th Floor Cheyenne, WY 82002 Phone: 307-777-8664 deanna.greene@wyo.gov	**h. Contract Officer:** N/A

FEES AND PRICING



Pricing

The testing fees are $37,812.01 including testing, reporting, and executive presentation. Please see attached Cost Worksheet.

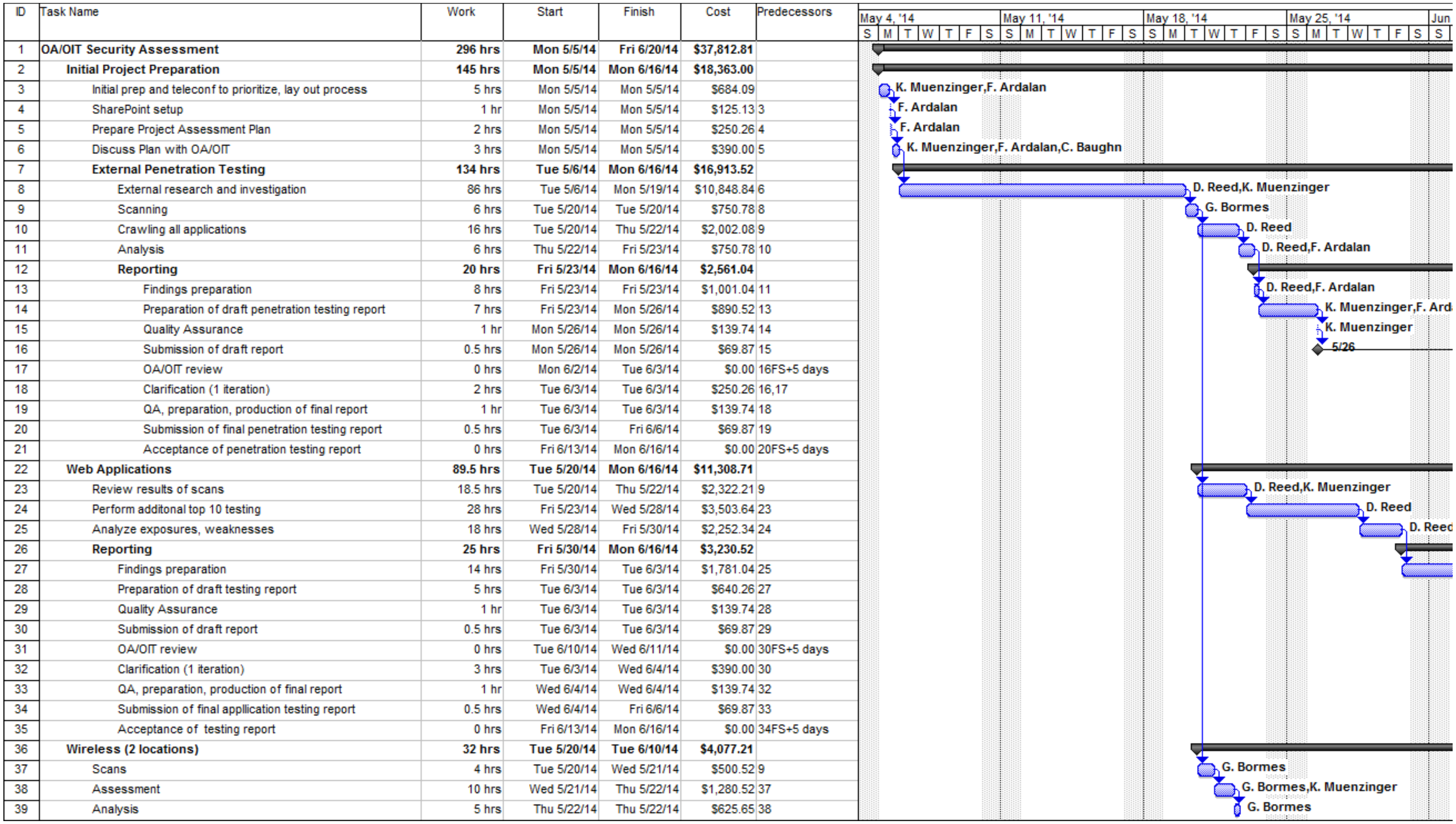
Invoicing

Invoicing will be as follows: 35% at the end of three weeks (roughly May 7); 30% at the end of May; 30% at the end of June; and 5% at completion of executive presentation.

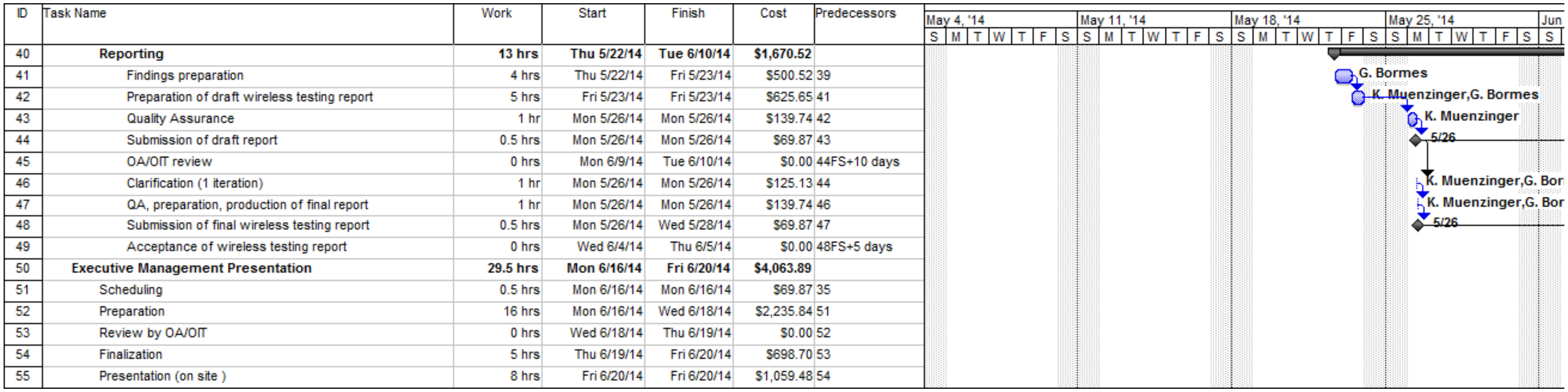
Project Work Plan

Utilizing a GANTT or PERT chart, include a high-level summary that shows all the tasks and deliverables to complete the project. Explain your approach to deliverables.

A small discrepancy exists between the attached Cost Worksheet and JANUS' Project Work Plan due to rounding. JANUS will accept the final cost as indicated on the Cost Worksheet - 37,812.01.



ID	Task Name	Work	Start	Finish	Cost	Predecessors
1	**OA/OIT Security Assessment**	**296 hrs**	**Mon 5/5/14**	**Fri 6/20/14**	**$37,812.81**	
2	**Initial Project Preparation**	**145 hrs**	**Mon 5/5/14**	**Mon 6/16/14**	**$18,363.00**	
3	Initial prep and teleconf to prioritize, lay out process	5 hrs	Mon 5/5/14	Mon 5/5/14	$684.09	
4	SharePoint setup	1 hr	Mon 5/5/14	Mon 5/5/14	$125.13	3
5	Prepare Project Assessment Plan	2 hrs	Mon 5/5/14	Mon 5/5/14	$250.26	4
6	Discuss Plan with OA/OIT	3 hrs	Mon 5/5/14	Mon 5/5/14	$390.00	5
7	**External Penetration Testing**	**134 hrs**	**Tue 5/6/14**	**Mon 6/16/14**	**$16,913.52**	
8	External research and investigation	86 hrs	Tue 5/6/14	Mon 5/19/14	$10,848.84	6
9	Scanning	6 hrs	Tue 5/20/14	Tue 5/20/14	$750.78	8
10	Crawling all applications	16 hrs	Tue 5/20/14	Thu 5/22/14	$2,002.08	9
11	Analysis	6 hrs	Thu 5/22/14	Fri 5/23/14	$750.78	10
12	**Reporting**	**20 hrs**	**Fri 5/23/14**	**Mon 6/16/14**	**$2,561.04**	
13	Findings preparation	8 hrs	Fri 5/23/14	Fri 5/23/14	$1,001.04	11
14	Preparation of draft penetration testing report	7 hrs	Fri 5/23/14	Mon 5/26/14	$890.52	13
15	Quality Assurance	1 hr	Mon 5/26/14	Mon 5/26/14	$139.74	14
16	Submission of draft report	0.5 hrs	Mon 5/26/14	Mon 5/26/14	$69.87	15
17	OA/OIT review	0 hrs	Mon 6/2/14	Tue 6/3/14	$0.00	16FS+5 days
18	Clarification (1 iteration)	2 hrs	Tue 6/3/14	Tue 6/3/14	$250.26	16,17
19	QA, preparation, production of final report	1 hr	Tue 6/3/14	Tue 6/3/14	$139.74	18
20	Submission of final penetration testing report	0.5 hrs	Tue 6/3/14	Fri 6/6/14	$69.87	19
21	Acceptance of penetration testing report	0 hrs	Fri 6/13/14	Mon 6/16/14	$0.00	20FS+5 days
22	**Web Applications**	**89.5 hrs**	**Tue 5/20/14**	**Mon 6/16/14**	**$11,308.71**	
23	Review results of scans	18.5 hrs	Tue 5/20/14	Thu 5/22/14	$2,322.21	9
24	Perform additonal top 10 testing	28 hrs	Fri 5/23/14	Wed 5/28/14	$3,503.64	23
25	Analyze exposures, weaknesses	18 hrs	Wed 5/28/14	Fri 5/30/14	$2,252.34	24
26	**Reporting**	**25 hrs**	**Fri 5/30/14**	**Mon 6/16/14**	**$3,230.52**	
27	Findings preparation	14 hrs	Fri 5/30/14	Tue 6/3/14	$1,781.04	25
28	Preparation of draft testing report	5 hrs	Tue 6/3/14	Tue 6/3/14	$640.26	27
29	Quality Assurance	1 hr	Tue 6/3/14	Tue 6/3/14	$139.74	28
30	Submission of draft report	0.5 hrs	Tue 6/3/14	Tue 6/3/14	$69.87	29
31	OA/OIT review	0 hrs	Tue 6/10/14	Wed 6/11/14	$0.00	30FS+5 days
32	Clarification (1 iteration)	3 hrs	Tue 6/3/14	Wed 6/4/14	$390.00	30
33	QA, preparation, production of final report	1 hr	Wed 6/4/14	Wed 6/4/14	$139.74	32
34	Submission of final appllication testing report	0.5 hrs	Wed 6/4/14	Fri 6/6/14	$69.87	33
35	Acceptance of testing report	0 hrs	Fri 6/13/14	Mon 6/16/14	$0.00	34FS+5 days
36	**Wireless (2 locations)**	**32 hrs**	**Tue 5/20/14**	**Tue 6/10/14**	**$4,077.21**	
37	Scans	4 hrs	Tue 5/20/14	Wed 5/21/14	$500.52	9
38	Assessment	10 hrs	Wed 5/21/14	Thu 5/22/14	$1,280.52	37
39	Analysis	5 hrs	Thu 5/22/14	Thu 5/22/14	$625.65	38



ID	Task Name	Work	Start	Finish	Cost	Predecessors
40	**Reporting**	**13 hrs**	**Thu 5/22/14**	**Tue 6/10/14**	**$1,670.52**	
41	Findings preparation	4 hrs	Thu 5/22/14	Fri 5/23/14	$500.52	39
42	Preparation of draft wireless testing report	5 hrs	Fri 5/23/14	Fri 5/23/14	$625.65	41
43	Quality Assurance	1 hr	Mon 5/26/14	Mon 5/26/14	$139.74	42
44	Submission of draft report	0.5 hrs	Mon 5/26/14	Mon 5/26/14	$69.87	43
45	OA/OIT review	0 hrs	Mon 6/9/14	Tue 6/10/14	$0.00	44FS+10 days
46	Clarification (1 iteration)	1 hr	Mon 5/26/14	Mon 5/26/14	$125.13	44
47	QA, preparation, production of final report	1 hr	Mon 5/26/14	Mon 5/26/14	$139.74	46
48	Submission of final wireless testing report	0.5 hrs	Mon 5/26/14	Wed 5/28/14	$69.87	47
49	Acceptance of wireless testing report	0 hrs	Wed 6/4/14	Thu 6/5/14	$0.00	48FS+5 days
50	**Executive Management Presentation**	**29.5 hrs**	**Mon 6/16/14**	**Fri 6/20/14**	**$4,063.89**	
51	Scheduling	0.5 hrs	Mon 6/16/14	Mon 6/16/14	$69.87	35
52	Preparation	16 hrs	Mon 6/16/14	Wed 6/18/14	$2,235.84	51
53	Review by OA/OIT	0 hrs	Wed 6/18/14	Thu 6/19/14	$0.00	52
54	Finalization	5 hrs	Thu 6/19/14	Fri 6/20/14	$698.70	53
55	Presentation (on site)	8 hrs	Fri 6/20/14	Fri 6/20/14	$1,059.48	54

Security Practices

As a security/recovery specialty firm, JANUS understands the need for protection of client materials. Within its headquarters location (where Commonwealth material will be kept), client materials are kept locked so that no client materials can be exposed to unauthorized users. All client-related materials are shredded prior to disposal and will be dealt with according to Commonwealth requirements as stated in the solicitation. Printed materials are in locked cabinets, not left in the open.

Since JANUS is a wholly-focused security company, each employee is much more attuned to security needs than is an average company's employees. No one needs to force JANUS employees to change passwords (or for them to be robust). Every person uses a proximity card badge as a matter of course every day. Electronic client materials are in a locked Data Center. JANUS operates in a Windows 2008 server environment with high levels of security implemented. Firewalls (that are regularly monitored and tested) prevent unauthorized outsiders from accessing files and appropriate access privileges prevent unauthorized insiders from the same.

In addition, all JANUS consultants work with encrypted laptops at client sites. Where "flash sticks" are utilized, these are also encrypted. The latest patches are applied prior to the laptops leaving the JANUS site. Typically, prior to leaving a client site, all client data are loaded into a protected repository through a secure portal and the laptop is cleaned. In this manner, client data are not subject to loss or theft. Although this is perhaps over and above requirements for vendors, JANUS takes its responsibility as a security company very seriously and understands that it has a responsibility to protect your information.

While transferring documentation and reports back and forth between client and JANUS, JANUS encourages use of its SharePoint portal which will be established for the Commonwealth at the beginning of the project. Thus, documents can be quickly checked in or out with version control to ensure security and speed.

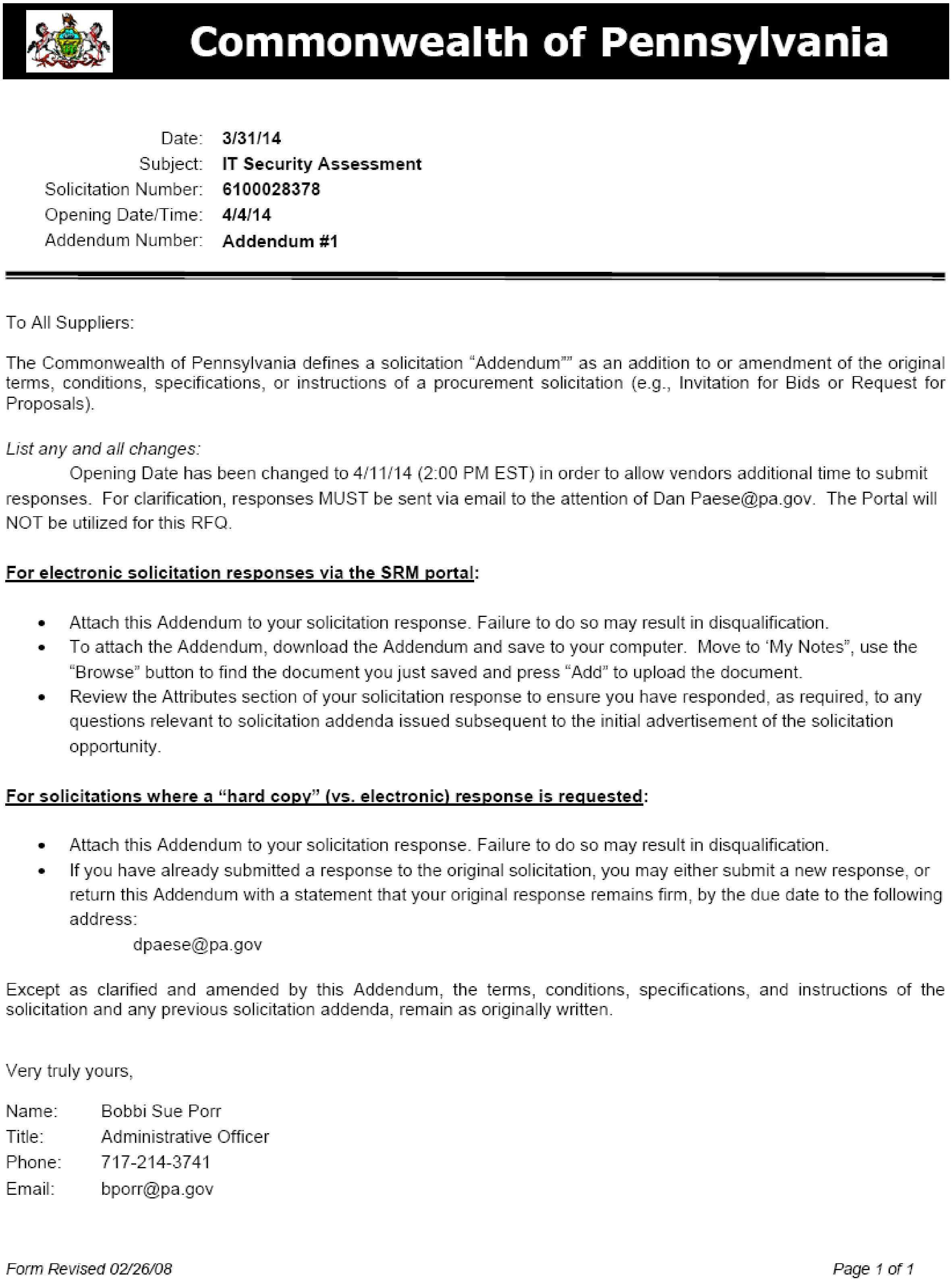
Bonding and Background Check Procedures

JANUS carries a criminal theft and fraud bond for $1,000,000. JANUS employees are bonded and undergo background checks (criminal and credit) prior to employment. JANUS also carries Errors and Omissions insurance as an additional level of protection for clients. Employees sign a five-page ethics statement upon entry to JANUS that defines their behavior and stresses that they are to put the needs of JANUS' clients first in all situations.

All employees have undergone background checks prior to their employment. In addition, all proposed employees have also undergone background checks by federal agencies and either hold, or are in the process of receiving U.S. Federal High Public Trust clearances for working with critical and sensitive data.

APPENDICES

Appendix A – Commonwealth's Addendum #1



Commonwealth of Pennsylvania

Date:	**3/31/14**
Subject:	**IT Security Assessment**
Solicitation Number:	**6100028378**
Opening Date/Time:	**4/4/14**
Addendum Number:	**Addendum #1**

To All Suppliers:

The Commonwealth of Pennsylvania defines a solicitation "Addendum"" as an addition to or amendment of the original terms, conditions, specifications, or instructions of a procurement solicitation (e.g., Invitation for Bids or Request for Proposals).

List any and all changes:

Opening Date has been changed to 4/11/14 (2:00 PM EST) in order to allow vendors additional time to submit responses. For clarification, responses MUST be sent via email to the attention of Dan Paese@pa.gov. The Portal will NOT be utilized for this RFQ.

For electronic solicitation responses via the SRM portal:

- Attach this Addendum to your solicitation response. Failure to do so may result in disqualification.
- To attach the Addendum, download the Addendum and save to your computer. Move to 'My Notes", use the "Browse" button to find the document you just saved and press "Add" to upload the document.
- Review the Attributes section of your solicitation response to ensure you have responded, as required, to any questions relevant to solicitation addenda issued subsequent to the initial advertisement of the solicitation opportunity.

For solicitations where a "hard copy" (vs. electronic) response is requested:

- Attach this Addendum to your solicitation response. Failure to do so may result in disqualification.
- If you have already submitted a response to the original solicitation, you may either submit a new response, or return this Addendum with a statement that your original response remains firm, by the due date to the following address:

  dpaese@pa.gov

Except as clarified and amended by this Addendum, the terms, conditions, specifications, and instructions of the solicitation and any previous solicitation addenda, remain as originally written.

Very truly yours,

Name:	Bobbi Sue Porr
Title:	Administrative Officer
Phone:	717-214-3741
Email:	bporr@pa.gov

Form Revised 02/26/08

Page 1 of 1

Appendix B – Client Comments

New York City

New York City, similar to many other government agencies, has a process for providing an official evaluation of its vendors at the conclusion of a contract. The process takes into account all elements of a project and a variety of individuals are canvassed for information. This report is filed in the NYC VENDEX system where all agencies can review a vendor's performance if they are contemplating doing business – so it is important to have a good rating.

JANUS completed a large security vulnerability assessment project focused on a New York City process focused on enabling businesses wishing to begin conducting business with that City to maneuver the complicated process of obtaining license, permits, and approvals. Termed the Business Express project it was a JANUS project from August 2010 – June 2011. JANUS received the official "report card" or performance evaluation on 9/9/2011. Of five available categories (moving from a "1" Unsatisfactory to a "5" Excellent), JANUS received an overall score of "5" Excellent. This takes into account quality of service, timeliness, and accountability.

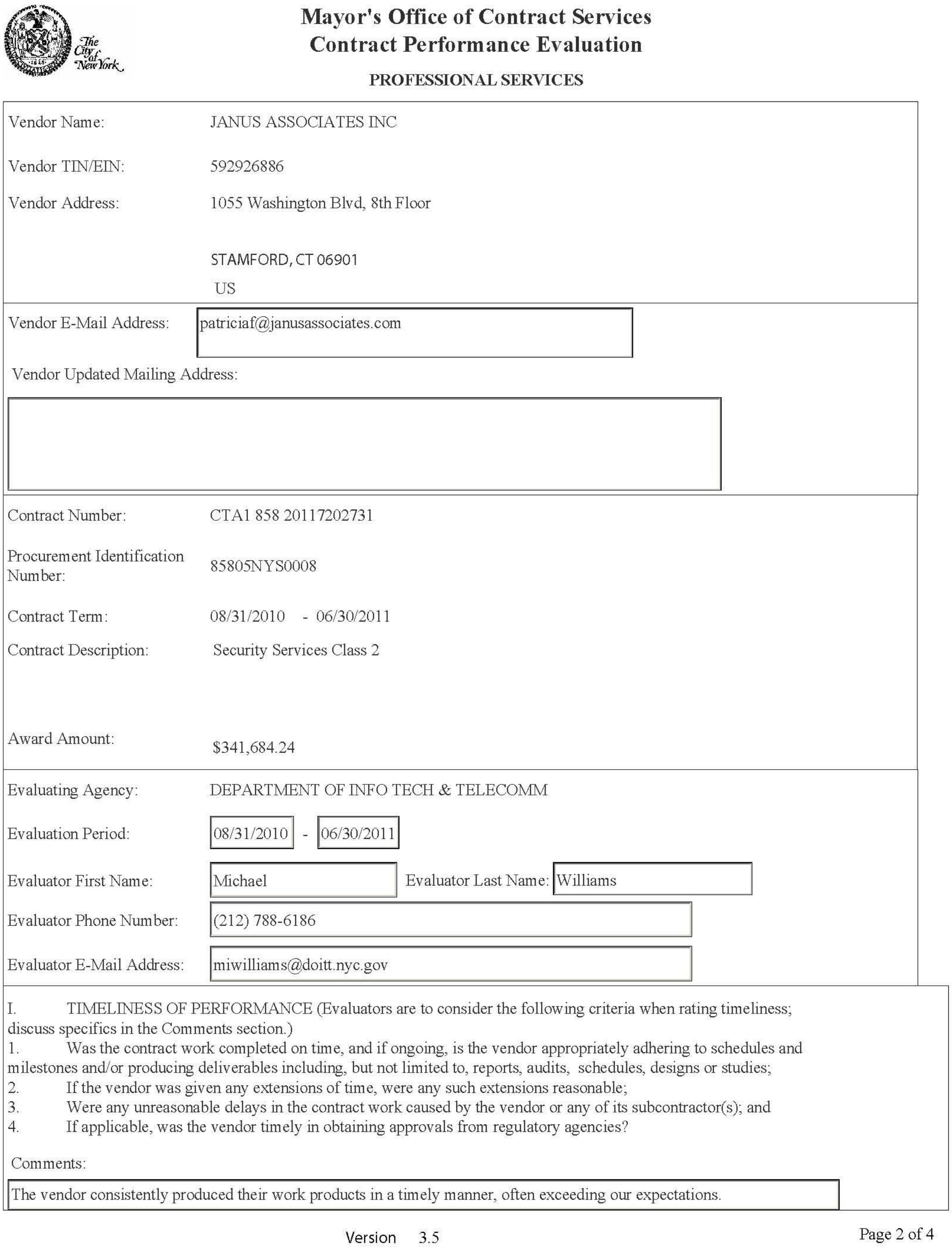
The City's official comments (now on-file) were as follows:

"The vendor consistently produced their work products in a timely manner, often exceeding our expectations."

"The vendor managed their costs in a way that was completely transparent, and consistently remained within budget."

"Overall, the vendor's performance was outstanding. They helped advise the project team of security issues and collaborate on remedial strategies, while also helping maintain excellent relations with DoITT's security team."

(See New York City submission on next pages.)



The City of New York

Mayor's Office of Contract Services
Contract Performance Evaluation

PROFESSIONAL SERVICES

Vendor Name: JANUS ASSOCIATES INC

Vendor TIN/EIN: 592926886

Vendor Address: 1055 Washington Blvd, 8th Floor

STAMFORD, CT 06901
US

Vendor E-Mail Address: patriciaf@janusassociates.com

Vendor Updated Mailing Address:

Contract Number: CTA1 858 20117202731

Procurement Identification Number: 85805NYS0008

Contract Term: 08/31/2010 - 06/30/2011

Contract Description: Security Services Class 2

Award Amount: $341,684.24

Evaluating Agency: DEPARTMENT OF INFO TECH & TELECOMM

Evaluation Period: 08/31/2010 - 06/30/2011

Evaluator First Name: Michael Evaluator Last Name: Williams

Evaluator Phone Number: (212) 788-6186

Evaluator E-Mail Address: miwilliams@doitt.nyc.gov

I. TIMELINESS OF PERFORMANCE (Evaluators are to consider the following criteria when rating timeliness; discuss specifics in the Comments section.)

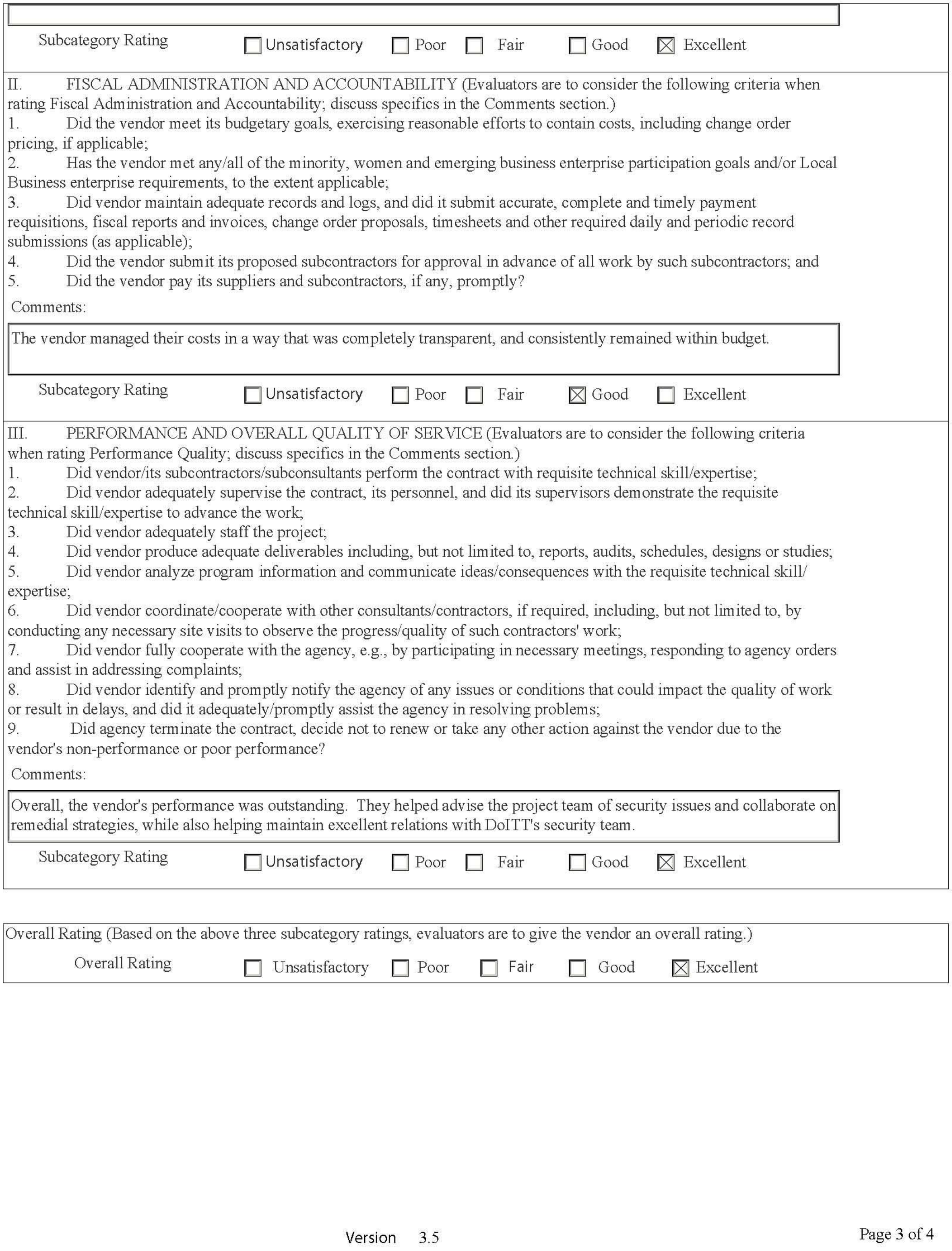
1. Was the contract work completed on time, and if ongoing, is the vendor appropriately adhering to schedules and milestones and/or producing deliverables including, but not limited to, reports, audits, schedules, designs or studies;
2. If the vendor was given any extensions of time, were any such extensions reasonable;
3. Were any unreasonable delays in the contract work caused by the vendor or any of its subcontractor(s); and
4. If applicable, was the vendor timely in obtaining approvals from regulatory agencies?

Comments:

The vendor consistently produced their work products in a timely manner, often exceeding our expectations.

Version 3.5

Page 2 of 4



Subcategory Rating ☐ Unsatisfactory ☐ Poor ☐ Fair ☐ Good ☒ Excellent

II. FISCAL ADMINISTRATION AND ACCOUNTABILITY (Evaluators are to consider the following criteria when rating Fiscal Administration and Accountability; discuss specifics in the Comments section.)

1. Did the vendor meet its budgetary goals, exercising reasonable efforts to contain costs, including change order pricing, if applicable;
2. Has the vendor met any/all of the minority, women and emerging business enterprise participation goals and/or Local Business enterprise requirements, to the extent applicable;
3. Did vendor maintain adequate records and logs, and did it submit accurate, complete and timely payment requisitions, fiscal reports and invoices, change order proposals, timesheets and other required daily and periodic record submissions (as applicable);
4. Did the vendor submit its proposed subcontractors for approval in advance of all work by such subcontractors; and
5. Did the vendor pay its suppliers and subcontractors, if any, promptly?

Comments:

The vendor managed their costs in a way that was completely transparent, and consistently remained within budget.

Subcategory Rating ☐ Unsatisfactory ☐ Poor ☐ Fair ☒ Good ☐ Excellent

III. PERFORMANCE AND OVERALL QUALITY OF SERVICE (Evaluators are to consider the following criteria when rating Performance Quality; discuss specifics in the Comments section.)

1. Did vendor/its subcontractors/subconsultants perform the contract with requisite technical skill/expertise;
2. Did vendor adequately supervise the contract, its personnel, and did its supervisors demonstrate the requisite technical skill/expertise to advance the work;
3. Did vendor adequately staff the project;
4. Did vendor produce adequate deliverables including, but not limited to, reports, audits, schedules, designs or studies;
5. Did vendor analyze program information and communicate ideas/consequences with the requisite technical skill/ expertise;
6. Did vendor coordinate/cooperate with other consultants/contractors, if required, including, but not limited to, by conducting any necessary site visits to observe the progress/quality of such contractors' work;
7. Did vendor fully cooperate with the agency, e.g., by participating in necessary meetings, responding to agency orders and assist in addressing complaints;
8. Did vendor identify and promptly notify the agency of any issues or conditions that could impact the quality of work or result in delays, and did it adequately/promptly assist the agency in resolving problems;
9. Did agency terminate the contract, decide not to renew or take any other action against the vendor due to the vendor's non-performance or poor performance?

Comments:

Overall, the vendor's performance was outstanding. They helped advise the project team of security issues and collaborate on remedial strategies, while also helping maintain excellent relations with DoITT's security team.

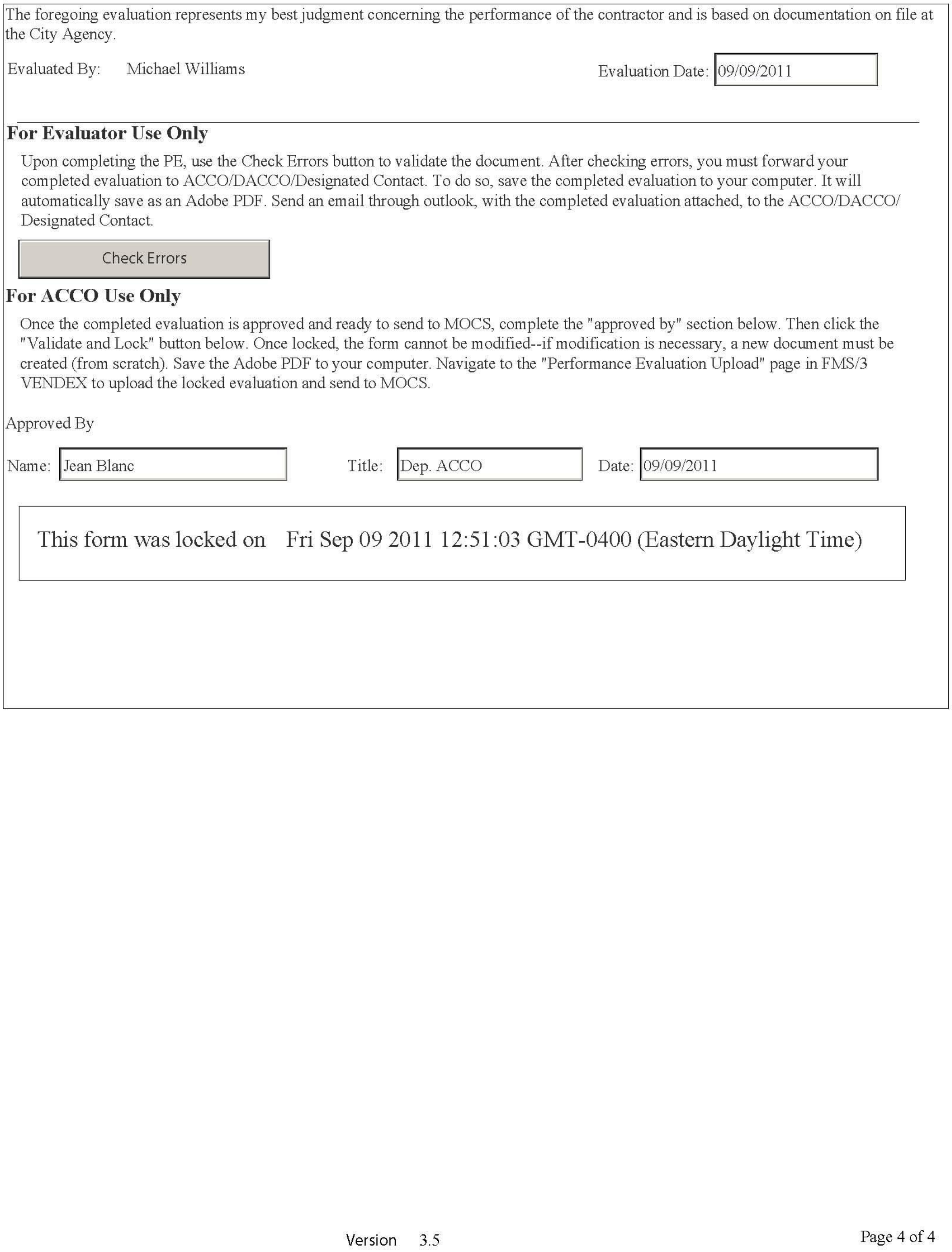
Subcategory Rating ☐ Unsatisfactory ☐ Poor ☐ Fair ☐ Good ☒ Excellent

Overall Rating (Based on the above three subcategory ratings, evaluators are to give the vendor an overall rating.)

Overall Rating ☐ Unsatisfactory ☐ Poor ☐ Fair ☐ Good ☒ Excellent

Version 3.5

Page 3 of 4



The foregoing evaluation represents my best judgment concerning the performance of the contractor and is based on documentation on file at the City Agency.

Evaluated By: Michael Williams

Evaluation Date: 09/09/2011

For Evaluator Use Only

Upon completing the PE, use the Check Errors button to validate the document. After checking errors, you must forward your completed evaluation to ACCO/DACCO/Designated Contact. To do so, save the completed evaluation to your computer. It will automatically save as an Adobe PDF. Send an email through outlook, with the completed evaluation attached, to the ACCO/DACCO/ Designated Contact.

For ACCO Use Only

Once the completed evaluation is approved and ready to send to MOCS, complete the "approved by" section below. Then click the "Validate and Lock" button below. Once locked, the form cannot be modified--if modification is necessary, a new document must be created (from scratch). Save the Adobe PDF to your computer. Navigate to the "Performance Evaluation Upload" page in FMS/3 VENDEX to upload the locked evaluation and send to MOCS.

Approved By

Name: Jean Blanc

Title: Dep. ACCO

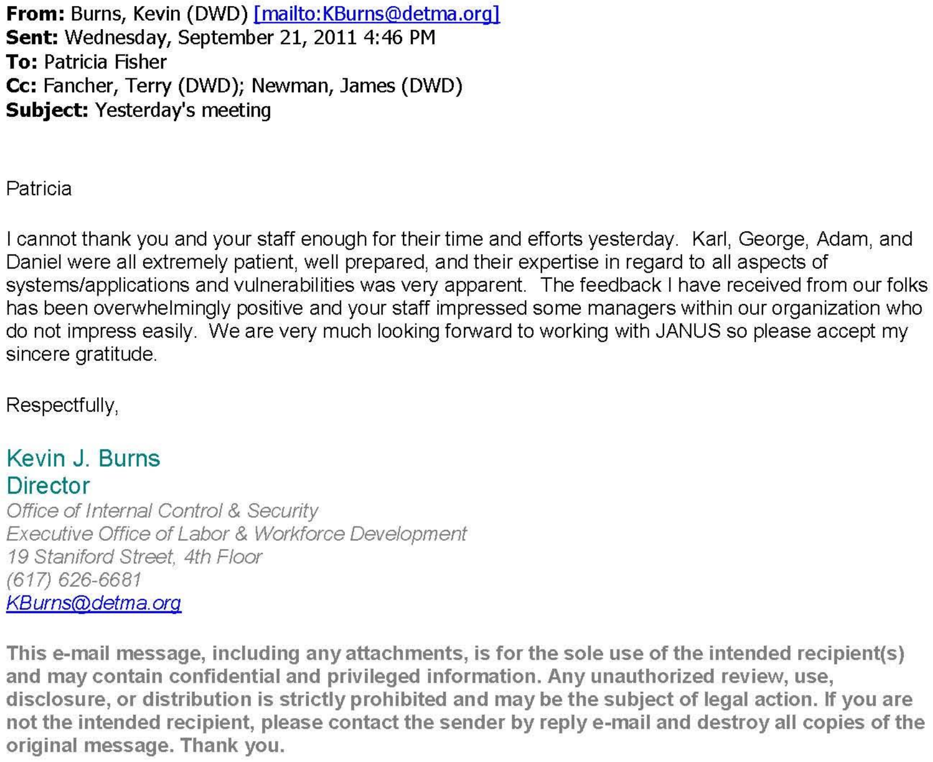
Date: 09/09/2011

This form was locked on Fri Sep 09 2011 12:51:03 GMT-0400 (Eastern Daylight Time)

Version 3.5

Page 4 of 4

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

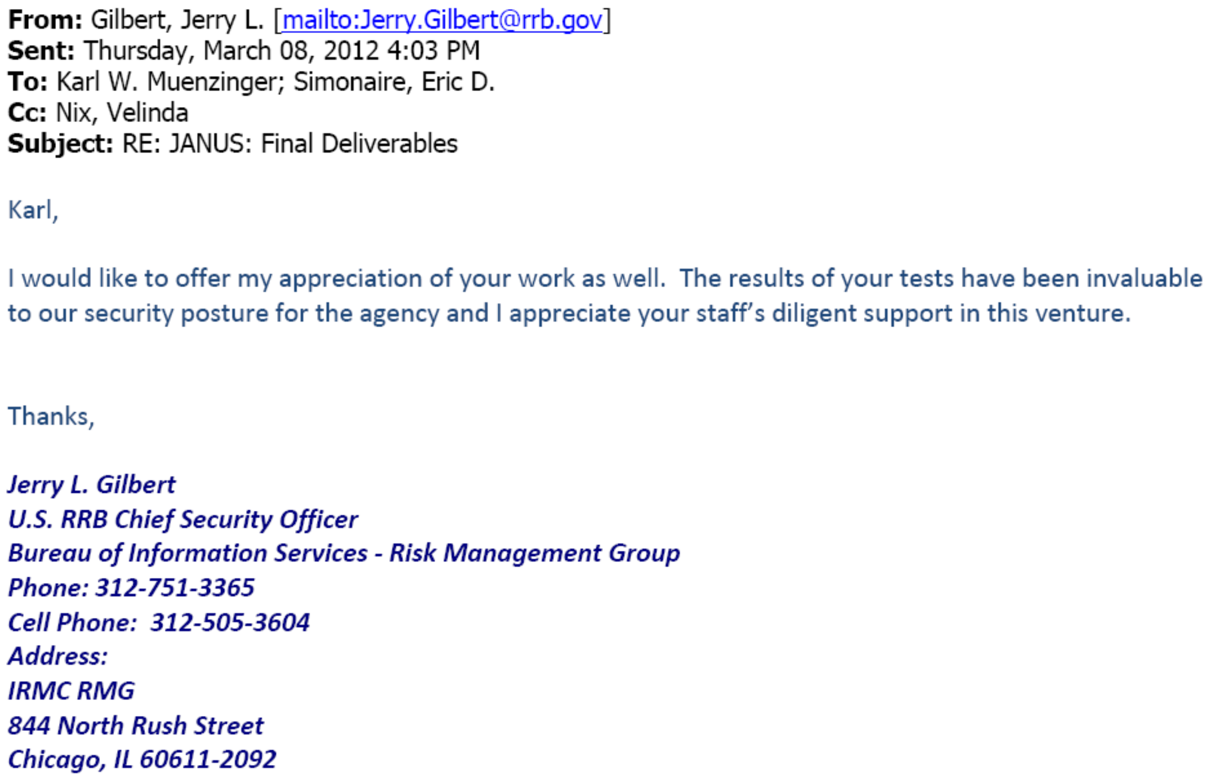
I cannot thank you and your staff enough for their time and efforts yesterday. Karl, George, Adam, and Daniel were all extremely patient, well prepared, and their expertise in regard to all aspects of systems/applications and vulnerabilities was very apparent. The feedback I have received from our folks 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.

U.S. Railroad Retirement Board



From: Gilbert, Jerry L. [mailto:Jerry.Gilbert@rrb.gov]
Sent: Thursday, March 08, 2012 4:03 PM
To: Karl W. Muenzinger; Simonaire, Eric D.
Cc: Nix, Velinda
Subject: RE: JANUS: Final Deliverables

Karl,

I would like to offer my appreciation of your work as well. The results of your tests have been invaluable to our security posture for the agency and I appreciate your staff's diligent support in this venture.

Thanks,

Jerry L. Gilbert
U.S. RRB Chief Security Officer
Bureau of Information Services - Risk Management Group
Phone: 312-751-3365
Cell Phone: 312-505-3604
Address:
IRMC RMG
844 North Rush Street
Chicago, IL 60611-2092

MBI Inc.

Client:	MBI Inc.
Assignment:	Penetration Test
Dates of Service:	4-9-12 – 5-7-12
Survey Completed by:	Tony Mastrofrancesco **Title:** IT Director – Technology & Security

Ratings:
5 = Outstanding 4 = Excellent 3 = Good 2 = Fair 1 = Poor

Rating	Review Area
5	Knowledge/Experience of JANUS Staff Performing the Work: The extent to which the knowledge/skills of JANUS consultants met the requirements of the work assigned Comments:
5	Quality of Product or Service: The extent to which JANUS work products met the contract's performance requirements Comments:
5	Cost Control: The extent to which JANUS managed costs according to contract requirements Comments:
5	Timeliness of Performance: The extent to which JANUS presented deliverables in accordance with contract requirements/client request Comments:
5	Business Relations: The extent to which JANUS responded effectively to inquiries and/or technical, service, administrative issues Comments:
5	Overall Customer Satisfaction: The extent to which JANUS demonstrated commitment to customer satisfaction Comments:
	Please X one: Overall, did JANUS Associates, ____ not meet, ____ meet or _x__ exceed your expectations: Comments:

Would you be willing to provide a reference letter?

Yes _x___ No ____

Would you conduct business again with JANUS Associates, Inc.?

Yes ___x_ No ____

Comments: George Bormes is a keeper. Easy to work with, knowledgeable, heads down worker.

Appendix C – Sample Deliverables

The following sample finding is from one of JANUS' recent reports. It has been redacted to protect JANUS' client's information, however, there is enough included for the Commonwealth to understand the JANUS approach and its attention to detail for its findings, as well as its thoroughness in presenting them.

Findings Format

The following represents the findings format typically followed by JANUS (this is from an actual finding).

#51 Business Risk: Weak Classification Procedures May Increase Risk of Information Disclosure

Priority: (Priorities Can Be High Risk, Medium Risk, Low Risk)

High

Ease of Fix: (Ease-of-Fix Can Be Easy, Moderately Difficult, Very Difficult, No Known Fix)

Moderate

Estimated Work Effort: (Estimated Work Effort Can Be Minimal, Moderate, Substantial, or Unknown.)

Unknown - If a classification process exists but is not being utilized, this may be able to be completed simply by informing XXXXX to begin using the system they document in the Security Plan.

If no classification system actually exists this could require approximately 80 hours to research and design.

Finding:

XXXXX indicates that data is classified as none, view only, or view and update. From the wording available indicating XXXXX intent, the use of this term is most likely incorrect. This appears to relate to system and user privileges, not data classification. We suspect that this causes user confusion regarding what their classification responsibilities are regarding how and what to classify. As a result, it is very likely that the classification schema is not relevant or being accurately used.

If this is intended to define data classification, another problem exists. No evidence of a data classification methodology being used for application information could be found during the review. We did find documentation labeled confidential but it was not particularly confined away from people. As a result, all information appears to have the same value. This certainly should not be true.

There are two problems that this causes. The first is that it is easy to incorrectly dispose of confidential information if it is not properly labeled. All data can look alike when printed. Without some manner of segregating confidential from unimportant information, there is no way to enforce proper handling.

When proprietary data are stolen one method of recourse is to sue in civil court even if criminal proceedings are not available. To do this successfully, one must prove damage. When data is not segregated according to its value with some written indicator (and cared for according to that legend), it is difficult to make the point that any piece of data is more or less valuable than any other. A file listing all the winning numbers can be interpreted by legal counsel to be no more valuable than an internal memo setting the time and place for the annual meeting. This problem has created difficulties for many organizations in the past when proprietary data have been stolen.

As a result of the lack of a data classification methodology and its consistent use, YYY and XXXXX would most likely lose a court case involving loss of proprietary data.

Recommendations:

1. Determine what data classification means in the XXXXX environment.

2. Ensure that a proper data classification methodology exists.

3. Enforce usage.

Sample Finding – Firewall Vulnerability

#43 Risk: xxx Firewall Is Susceptible to a Denial-of-Service Attack

Priority: (Priorities Can Be High Risk, Medium Risk, Low Risk)

High Risk

Ease of Fix: (Ease-of-Fix Can Be Easy, Moderately Difficult, Very Difficult, No Known Fix)

Moderately Difficulty

Finding:

COSMO.xxxxxxxxxx.COM (xxx.xx.x.xx) is susceptible to a denial-of-service attack that will crash the Firewall. See the following message from Checkpoint regarding this DOS attack. Although this message implies that the risk of a successful Denial-of-Service attack against the un-trusted interface is small, there have been several reports on the Internet of successful attacks launched against the un-trusted interface of a Check Point Firewall.

Check Point is aware of a published Denial-of-Service attack against the Check Point connection table, used by Firewall-1, FloodGate-1 and VPN-1. For additional information on the attack, see http://www.securityfocus.com/vdb/bottom.html?vid=549. The remainder of this message describes the attack, its practical impact, ways to mitigate, and the steps Check Point is taking to eliminate the attack.

When a Check Point gateway receives a packet that is not registered in its connection table and is not otherwise allowed (e.g. expected FTP data connection) or prohibited (e.g. SAM blocked) it will try to match it to the rule base. Specifically, when a "unfamiliar" TCP ACK packet is received it will be matched against the rule base and if an accept rule is found it will be recorded in the connection table, because this is a packet in an "established" connection (in the context of TCP) the timeout will be set to the TCP timeout that is defined in the policy configuration properties (3600 seconds by default).

If enough such packets are sent the connections table may fill up and the connectivity through the gateway may suffer. Note that only packets that are allowed by the rule base can be added to the connections table in this manner. This means that for "inbound" packets (i.e., from the Internet) the destination must normally be a well-known server behind the gateway. This server will immediately send a TCP RST packet, which will decrease the timeout in the connections table to a smaller timeout (50 seconds by default), this will make it much harder to saturate the connections table.

For "outbound" packets (i.e., going to the Internet) rules are likely to be less restrictive and the possibility is much higher of addressing a non-existent server (thereby avoiding a RST and transition to a smaller timeout).

This Denial-of-Service attack depends on the Ability to send enough ACK packets within a certain time period. This is far likelier from the inside, with its relatively higher access speeds (being LAN connected) to the target gateway, than from the Internet side.

Therefore, Check Point sees the primary risk of this attack to be from malicious insiders, attempting to deny external connectivity to others within the organization.

Possible ways to minimize the vulnerability:

1. Craft a rule base that reduces Ability to insert ACK packets into connections table. For example:

➢ Minimize ACCEPT rules with destination ANY, one option is to add Client Authentication (with concurrent session limits).

➢ For those services that use ACCEPT to destination ANY, consider the use of Fast Mode (V4.0) on that service (there are limits on the user of Fast Mode in conjunction with NAT, encryption and other features, please consult the Firewall-1 documentation).

2. Increase the size of the connections table, in order to increase the number of ACKs needed to affect connectivity. To do this (assuming V4.0) perform the following:

➢ Edit $FWDIR/lib/table.def. The attribute limit followed by the limit value (for instance, limit 50000 for 50000 connections), should be inserted after hashsize 8192 attribute of the Connection Table. It must be inserted at the two locations, within $FWDIR/lib/table.def file (the two lines which begin with "connections = ").

Example:

```
connections = dynamic refresh expires TCP_START_TIMEOUT   expcall       KFUNC_EXPIRE
implies    tracked kbuf 1 hashsize 8192   limit 50000;
```

➢ Note that increasing the hashsize value might be needed to maintain performance. Hashsize should be a power of 2, and its value should be as approximate number as possible to the limit value. For example, if the limit value is 50,000, hashsize should be 65536.

➢ Validate that enough memory has been allocated to the Check Point kernel to handle the increased connections table. Using a general rule of: connection table size = ([memory] - X)/60, where X should be a value between 0.5-3 Mbytes (depending on the amount of logging and accounting done by the Firewall), and [memory] is the internal memory allocated for the Firewall-1 (use $FWDIR/bin/fw ctl pstat to get this number). If the connection table size is less than your desired limit, you may need to increase kernel memory. Please see Page 372 in the Firewall-1 4.0 Architecture and Administration User Guide on how to increase the memory allocated to the Firewall-1 kernel (the method is OS dependent).

3. Reduce the default TCP timeout to a low enough value that will be lower than the time it takes to fill the connections table. This has the disadvantage that low activity sessions (e.g., Telnet) may timeout. In case of using NAT hide, this will mean losing the connection.

Check Point is in the process of validating an INSPECT code change that will cause unknown TCP ACK packets to be dropped prior to matching them with the rule base. This change, will be available for both V3.0 and V4.0 versions, and will post to the Check Point web site, and to the FireWall-1 Mailing List. The disadvantage of this INSPECT fix will be that following a reboot, policy unload or stopping the Firewall,

all active TCP connections will be blocked, and that any timed out TCP connections (i.e., connections that have been inactive longer than the TCP timeout) will be disconnected. The behavior with regards to maintaining connections after policy reload will not be affected by the change.

In summary: while flooding a Check Point gateway with acceptable ACK packets may fill the connection tBBDle and have adverse connectivity effects, vulnerability is most realistically from users on the internal side of the gateway and there are simple measures that can be taken to minimize it. In addition, Check Point is taking steps to supply an INSPECT script that should eliminate this problem for those customers that view this as a significant vulnerability.

Recommendations:

1. Make the recommended changes to COSMO.
2. Contact Check Point to determine if a permanent solution to this vulnerability exists.

Estimated Work Effort: (Estimated Work Effort Can Be Minimal, Moderate, Substantial, or Unknown.)

Estimate – eight hours

End of Document