RFP 21-68067 Security Controls Audit Services
Attachment F Technical Proposal

Instructions: Please provide answers in the yellow shaded areas ONLY to all questions. Reference all attachments in the shaded area.

General

2.4.1 Please provide a brief history of your organization's experience with providing security control audit services.

JANUS is an independent, privately-owned information security specialty consulting/audit/ assessment company headquartered in Connecticut and is the longest operating cyber and data 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 32 years due to the excellence of our offerings, our dedication to our clients, our vendor neutral results, and our ability to compete successfully with the largest security organizations. JANUS focuses on information security, business resilience, IT needs assessments/audits and strategy as well as associated services as its core business and possesses all the depth and experience required to fulfill the Lottery'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 Lottery discover risks early and then making practical recommendations for mitigating them is one of the best ways we can add value to your operation, protect it, and get you on the path to 2020 WLA-SCS certification, if you wish as well as ISO 27001 certification. We believe our high standards and complimentary skill sets will exceed your expectations for this security project.

JANUS is not affiliated with any hardware or software providers. Therefore, you can be assured that we have no relationships which would influence our recommendations. Even though we have experience with the security requirements of many types of products and equipment and understand them well, we are totally focused on your needs. We do not receive revenue from any vendors; therefore, you will receive unbiased recommendations from us.

The JANUS approach has been well-honed by many similar assessments and penetration tests 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 Lottery will receive greater value for its expenditure, thus in turn, providing even greater worth to your customers.

A cornerstone of a JANUS audit or test is our explanation of business risks related to technical or process and operational issues. Every JANUS finding carries with it a delineation of the actual risk to 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.

To provide a clearer understanding of JANUS' relationship with our clients and high-quality deliverables, we include the following comments made by our clients.

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

Wyoming State Agency

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

Massachusetts State Agency

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

Federal Agency

Question #/Question	**Rating**
9. Rate the knowledge of the vendor's assigned staff and their ability to accomplish duties as contracted.	**RATING: 10**
Comments: Janus has a veteran staff that saw very little turnover. Key personnel remained on the project throughout each project. Over the eleven years that I worked with Janus, key personnel left on the rare occasion due to health reasons or changes in their personal lives that required a physical move. Often, they still remained on the project assisting with the completion remotely. New experienced staff was brought on board to continue Janus' quality of service. In addition, the staff has experience across all levels of information security from the mainframe, mid-tier, desk-top to all current mobile and network technologies. This was particularly important in an agency that employs all of the above. Janus' management style is very hands-on and regularly met to discuss the project status and make any necessary adjustments based on the technical direction of the Project Officer.	

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

JANUS has provided security/risk/vulnerability assessments/audits, penetration tests, and gap analyses for a variety of large, critical institutions and lotteries/gaming operations. In addition, we regularly perform assessments and penetration tests for both U.S. federal agencies and a wide variety of states.

JANUS' long commitment to information security and business continuity with lotteries, gaming organizations, and other complex organizations has provided our consultants with a high-level of understanding of gaming regulations as well as with organizations servicing them such as IGT, formerly GTECH. This knowledge has been essential in establishing JANUS' standing in both the cyber security and the gaming fields. JANUS consultants also have been described by clients such as Charles Schwab as world-class and are often called upon to speak publicly. 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 Appendix D of this proposal.

JANUS has also completed security penetration test and vulnerability assessment projects for a variety of states including New York, Maryland, Virginia, Massachusetts, Minnesota, North Carolina, South Carolina, Texas, Vermont, Wyoming, Wisconsin, and Washington as well as many commercial enterprises throughout the U.S. and abroad. It is this expertise that has led a number of large critical infrastructure organizations to seek out JANUS for security assessments, audits, and penetration tests.

Because of our 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.

A sample group of JANUS' security consulting clients includes Gaming/GTECH clients such as:

- Minnesota State Lottery
- Mohegan Sun Casino
- Navajo Nation
- Gila River Hotels and Casinos
- Massachusetts PCI with GTECH
- Capital District Transportation Authority
- Oregon State Lottery
- Connecticut State Lottery Corporation

State/county/city government organizations such as:

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

- State of Wisconsin
- Washington State
- State of Wyoming
- Broward County (FL)
- Charles County (MD)
- Howard County (MD)
- Putnam-Westchester County (NY)
- Madison County (IL)
- Naperville (IL)
- New York City
- Baltimore County

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)
- Federal Reserve Board (FRB)
- Railroad Retirement Board (RRB)

Healthcare clients such as:

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

Insurance clients such as:

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

Education clients such as:

- Charles County Public Schools (Maryland)
- Wor-Wic Community College (Maryland)
- College of Southern Maryland
- Frederick County Public Schools (Maryland)
- Sailor Network (Maryland educational and library backbone network)
- Texas State Technical College
- Texas Tech University Health Sciences Center
- University of Texas

- State University of New York Buffalo
- Harford County Public Schools (Maryland)
- Community College of Baltimore County
- Mohawk Valley Community College (New York)
- Anne Arundel Community College (Maryland)
- Prince George's Community College (Maryland)
- California State University at Sacramento
- Sacred Heart University
- University of Wisconsin-Madison
- University of California at Berkeley
- The McCormack Institute of the University of Massachusetts
- University of Central Arkansas

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.)

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

JANUS CAPABILITIES

Founded in 1988, JANUS is America's longest operating information security firm. JANUS specializes in protecting our clients' data and computing environments through:

- Security and risk assessments/audits;
- Penetration tests;
- Infrastructure security testing;
- Information security support;
- Assurance and certification;
- Gap analyses;
- Quality assurance;
- Independent Verification and Validation;
- Current-State/Future-State assessments;
- Security Learning Management Systems and content;

- Data forensics;
- Compliance needs; and
- Business continuity.

JANUS also utilizes all the above types of focus needs in assisting our clients to transform their IT governance environments to meet future needs through IT Current-State/Future-State assessments, costing, benchmarking, Roadmap development, and virtual Chief Information Security Officer advisement as well as governance issues designed to define meaningful dashboards with which to report performance against goals.

JANUS' long commitment to improving infrastructure, IT security, data, and compliance has resulted in our 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 our 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 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 our first major enterprise-wide engagement by conducting a comprehensive, multi-facility review and vulnerability assessment of mainframe and server 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 outdated, lost and/or stolen hardware/software. Southern New England Telephone (now AT&T) had JANUS audit 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 us the ideal candidate for security management assignments. JANUS staff, through our many projects, has gained a strong understanding of the issues confronting our clients' needs and desired goals; the problems that might occur during projects; the way to structure tasks to ensure they are controllable; and the management of a variety of simultaneous subtasks. As a result, JANUS projects are completed on-time and on-budget.

E-Commerce

As Internet usage increased in both business and industry, JANUS responded to clients' e-commerce needs. Adding people to our staff who had been involved in some of the first Internet security incidents reported to the FBI, JANUS consultants were able to address increasingly complex e-commerce and Internet issues. JANUS currently provides services such as 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.

We continue to serve a wide range of clients in government and industry and bring the best practices of both sectors to our projects.

2.4.2 Please identify the industry accepted standards that will be used during the audit (IT, operational, accounting, etc.)

The Lottery has requested that JANUS' work focus on both ISO 27001 and the World Lottery Association Security Control Standard to position the Lottery for Certification Level 2. Therefore, JANUS will assess to those standards.

Project Plan

2.4.3 Please provide resumes of all key team members planned to be part of the engagement, including their involvement on similar engagements. Also identify how the team will be organized, while demonstrating that sufficient resources exist to conduct the services being requested within this RFP.

JANUS has more than adequate resources to undertake this audit. We are actually presenting additional team members than we need, in case timing issues require additional staffing. We also have two specialty certified small business subcontractors who will be assisting; one focusing on physical security and one handling procedural auditing including interviews locally to the Lottery. JANUS staff will perform the major portion of the audit.

The team will be organized under the direction of [Redacted] with the technical elements led by [Redacted], although all reporting will be the responsibility of [Redacted], with assistance by [Redacted]. Oversight will be by Patricia Fisher, CEO of JANUS, who will focus on quality of results and customer satisfaction. Please see organization chart provided below.

[Redacted]

Resumes are provided in Appendix A.

2.4.4 Please explain in detail the proposed audit plan describing the specific steps that will be performed as part of the audit, including a list of deliverables that will be included. Please include audit objectives, control objectives, audit procedures used to conclude upon objectives, staff members assigned, and hours proposed for each audited area. The audit areas are listed in Section 1.4.A Summary Scope of Work of the RFP.

METHODOLOGY AND APPROACH

We outline, in the following sections, our approach and how we anticipate structuring the project and implementing the steps of the tasks so that we follow a logical progression.

Proposed Project and Audit Objectives and Plan

Audits such as this are a specialty of JANUS'. From our many years of experience and having worked with a large number of organizations, we understand the significant issues that government institutions and gaming/lottery operators must manage – particularly the need to be inclusive for the citizenry yet still protect and have the security infrastructure to do so. We understand these types of projects and, although we have developed a thorough methodology that has been honed from many hundreds of similar tasks over our 32-year history, we also offer flexibility in meeting your standards. Since we sell no products or software, we will provide an independent perspective with no conflicts of interest that might result from any other involvement with the Lottery.

[Redacted]

[Redacted]

[Redacted]

Approach

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

Blended Methodology

[Redacted]

Team Effort and Knowledge Transfer

[Redacted]

[Redacted]

[Redacted]

Technical Currency and Results

[Redacted]

Independent Manual Verification

[Redacted]

[Redacted]

Technical Testing

[Redacted]

Technical Testing Methodology

[Redacted]

[Redacted]

Preliminary Activities

[Redacted]

[Redacted]

Entry Meeting

[Redacted]

Post-kickoff Activities

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

[Redacted]

Communications Plan

[Redacted]

[Redacted]

Penetration Testing of Lottery Network

[Redacted]

[Redacted]

“[Redacted]” or “[Redacted]” Testing

[Redacted]

[Redacted]

We utilize a variety of testing and scanning tools for penetration testing tasks such as this. Which ones we will utilize in this project will depend on how far into the Lottery environment we can penetrate (please see Appendix B for sample of our major tools). We also are utilizing additional, specialized tools in recent tests such as:

[Redacted]

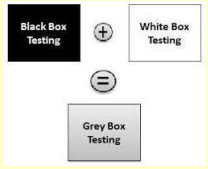
[Redacted]

"[Redacted]" Review[1]

[Redacted]

A wide variety of issues are investigated, and at a minimum, the following are utilized:

[Redacted]



Information Systems Security

[Redacted]

[1] Where applicable.

[Redacted]

[Redacted]

[Redacted]

[Redacted]

Policies and Procedures

[Redacted]

Wireless Assessment

[Redacted]

[Redacted]

Draw Game Drawings Security

[Redacted]

We anticipate performing this portion of the audit on-site, during a drawing.

(**Optional**)

[Redacted]

[Redacted]

Business Continuity Planning of the Hoosier Lottery

[Redacted]

[Redacted]

Best Practices of Lottery Potential Fraud Investigation Practices

[Redacted]

Security Department Management, Duties and Procedures

[Redacted]

[Redacted]

2.4.5 Please provide a timeline indicating when each phase of the engagement will be completed, including important milestones.

This is simpler to illustrate than explain. Therefore, we have prepared a preliminary project plan which we are enclosing that illustrates each of the steps we plan to include and the timing and resources for each.

	Task Name	Work	Start	Finish	Predecessors
1	**Security Project**	**485 hrs**	**Mon 7/26/21**	**Mon 9/20/21**	
2	Project award	0 hrs	Mon 7/26/21	Mon 7/26/21	

3	[Redacted]				
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					
18					
19					
20					
21					
22					
23					
24					
25	[Redacted]				
26					
27					
28					
29					
30					
31					
32					
33					
34					
35					
36					
37					
38					
39					
40					
41					
42					
43					
44					
45					
46					
47					
48					
49					
50					
51					
52					
53					
54					
55					

56	[Redacted]				
57					
58					
59					
60					
61					
62					
63					
64					
65					
66					
67					
68					
69					
70					
71					
72					
73					
74					
75					
76					
77					
78					
79					
80					
81					
82	[Redacted]				
83					
84					
85					
86					
87					
88					
89					
90					
91					
92					
93					
94					
95					
96					
97					
98					
99					
100					
101					
102					
103					
104					
105					
106					
107					
108					
109					
110					
111					
112					

113	[Redacted]				
114					

Project Close Out/Completion

2.4.6 Please describe in detail how your organization will analyze and summarize the results of your findings.

Gap Analysis

[Redacted]

Deliverables

[Redacted]

Audit Plan

[Redacted]

[Redacted]

[Redacted]

Preliminary Draft and Briefing

[Redacted]

Final Reports

The final report is prepared shortly after receiving management comments in preparation for the final report.

Briefing

We will provide a final briefing for your Executive Director (and/or designated staff) at the conclusion of the project.

Status Reports

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

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 Lottery staff accompanied by high levels of security – or we can specifically deliver them.

2.4.7 Describe in detail how your organization will provide recommendations for improving current processes where deficiencies have been identified.

[Redacted]

Subcontractor Information

Attachment E – Business Proposal, Section 2.3.9 Subcontractors states the following: "…the technical proposal must include the identification of the functions to be provided by the subcontractor and the subcontractor's related qualifications and experience." This information is provided below.

Process and Procedures for Compliance Auditing

RADcube's risk and compliance auditors will utilize ISO 27001 and the World Lottery Association industry standards for Information Security Management System (ISMS) for the assigned compliance and on-site interviewing tasks intended to further your information security needs. RADcube is an experienced Indiana information security firm that has conducted and delivered compliance projects for organizations and government agencies maintaining the security, integrity, compliance, and availability of their critical IT assets with a proven record of industry leading innovations. Radcube understands what is needed for this project and under JANUS' overall project guidance will provide the detailed findings of non-compliant areas and systems that the Lottery requires.

Physical Security

FireWatch Solutions, Inc. is well versed with conducting physical security assessments taking a holistic view of the human and technical elements that make up a protective posture. Integrating special operations and private security experience, our employees understand the multifaceted components required to keep facilities and personnel safe in a fluid risk environment. FireWatch examines the full spectrum of physical security to include:

- Screening, vetting, and onboarding of new security staff
- Policies, procedures, and protocols
- Security staff training levels
- Access control measures, perimeters, barriers
- Camera surveillance systems
- Security lighting
- Environmental systems
- Emergency response systems
- Sensitive material storage
- Liaison with external agencies
- Business continuity plans/data backup plans

Appendix A – Resumes

Function and Specialization
Executive Oversight Management

- IT Governance
- Project Management
- Strategic Analysis
- Risk Management
- Security Analysis/Assessment

Clearance
Top Secret Clearance – Inactive

Representative Clients
Commonwealth of Massachusetts
Centers for Medicare & Medicaid Services
Community Health Network of Connecticut
Commonwealth of Pennsylvania
Capital District Transportation Authority
City of Naperville (IL)
Wicomico County Public Schools (MD)
Travis County (TX)

Certification(s)
CGEIT – Certified in the Governance of Enterprise IT (ISACA)
CRISC – Certified in Risk and Information Security Controls (ISACA)
CDPSE – Certified Data Privacy Solutions Engineer
MBCI – Member, Business Continuity Institute

Patricia A. P. Fisher

Background
Ms. Fisher has 32 years with JANUS where she specializes in both the governance of Information Technology and information security and risk management projects, providing analysis and strategic advice to executive boards and leadership teams of JANUS' clients. Her time with JANUS was preceded by 11 years at IBM as Country Manager, Information Security & Business Continuity for Latin America and Canada. Prior to that she also managed large corporate Data Centers for IBM as well as large-scale application development projects. She has led a wide variety of projects over many years for government entities and not-for-profit customers, and is a highly sought after speaker and writer of articles. Ms. Fisher is a former member of the New York City Housing Authority's Audit Committee and served as the IT expert for the Committee.

Experience
JANUS Software, Inc. (d/b/a JANUS Associates) **December 1988 – Present**

- Completed security process improvement project for large transit authority.
- Performed CISO services for regional healthcare firm to assist it to drive needed security programs.
- Conducted high level strategic Information Technology review of state contractor firm to assist in developing budget, setting priorities, analyze staffing, and determine comprehensiveness of policies and procedures.
- Project oversight manager of Current-State/Future-State IT assessment for large state agency.
- Project oversight executive for major Independent Verification and Validation project for State Department of Revenue.
- Project oversight executive for information security contract for large federal healthcare organization.
- Advises senior executives at Fortune 100 companies and federal agencies on IT risk, staffing, and security initiatives.
- Led major corporate business and technology IT technical and business justification projects.
- Advised insurance clients on HIPAA, IT security requirements.
- Formulated and led team to design biometric identity management product.
- Designed Risk Management programs, methods for large organizations.
- Managed establishment of Risk Management program for federal agency.
- Advised senior security management of large financial institutions on corporate governance, organizational structure.
- Managed large information security projects for various public and private clients.

Education

B.A., Economics, (Maxwell School) Syracuse University

M.B.A., Marketing, Syracuse University

Post Masters Computer Science and Doctoral Studies, Pennsylvania State University & State of New York at Albany

- Designed and provided executive and employee training throughout U.S. for large television/news organization.
- Defined and oversaw execution of technical IT business justification process for large commercial financial organization.
- Performed one-on-one executive information security tutoring for large corporations.
- Performed agency-wide information security strategic program review for large federal health agency.
- Defined information technology/security strategies for various large client organizations.
- Designed and performed information security training sessions for corporate clients.
- Developed standardized risk assessment evaluation methodology for federal healthcare agency.
- Managed general support system and application HIPAA system control assessment process for CMS.
- Led security risk assessments/penetration tests for major multi-national and government clients.
- Performed Business Impact Analyses for Fortune 100 corporations, large banks, brokerages.
- Led security penetration tests and vulnerability analyses for international and U.S. clients.
- Completed Disaster Recovery Plans to fulfill prime contractor requirements for federal agency systems.
- Performed security/recoverability audit for international bank.
- Advised clients on improvements in security awareness programs; developed tools/techniques for training.
- Developed software sensitivity certification and governance process for NASA's International Space Station project.
- Conducted certifications of adequacy of Commercial-off-the-shelf and custom software/systems to meet NASA security/recovery criteria for contractors.
- Managed security sensitivity certification process for large federal prime contractor.
- Designed continuity test plans for various clients and monitored test execution.
- Conducted risk analyses, policy and procedure development, education, business continuity planning for commercial and governmental organizations.
- Performed strategic security administration study for Fortune 100 insurance firm.

International Business Machines, Inc. **August 1977 – December 1988**

Information Security Program Manager

- Performed critical consulting role during planning and justification of major disaster recovery proposal that resulted in present IBM hot-site offering.
- Consulted with key international and domestic IBM customers regarding recovery needs, information security problems.
- Conducted U.S.-wide fraud audit resulting in criminal prosecution.
- Managed international information security program for IBM internal Latin American sites.
- Designed and conducted international training programs for information security initiatives.
- Advised senior level executives on country/site security status throughout Latin America and Canada.

- Directed short-term assignees from Latin countries.
- Supervised budget/financial aspects and risk management of international program.
- Developed measurement techniques to achieve proper level of control.
- Designed series of security metrics to measure improvements in IBM program.
- Developed strategic/business focus for America's Group advising on security and selling IBM approach.
- Structured disaster recovery offerings to market to key customers (domestic and Latin).
- Provided security consulting services for IBM key customers.
- Conducted customer educational seminars for senior executives, staffs and information security personnel.
- Managed multi-divisional financial planning, product inventory, and pricing applications.
- Managed financial accounting Information Technology services for largest IBM division.
- Performed technical assessment and final financial approval for multi-divisional capital requests (in excess of $230 million per quarter).
- Revised methodology for quarterly capital investment process resulting in release of dollars to the IBM divisions.
- Operated large headquarters data center, 107 staff upon completion of assignment (operations, systems support, networking, information center, etc.).
- Managed staffing reduction of 25% over three years while consistently achieving 99.9% availability with sub-second response to 1800 users.
- Directed planning requirements for new IBM major computer center site.
- Managed data center recovery programs.
- Divisional management of United Way campaign – achieving highest participation/contribution rate ever in IBM while managing to lowest expenditure in the entire corporation.
- Designed state-of-the-art computer command center off raised floor.

Other Experience and Professional Accomplishments

Professional Education

Goldman Sachs 10,000 Small Businesses Graduate
IBM President's Class
IBM Advanced Middle Manager's Class
IBM Advanced Business Institute

Awards, Honors, Service

Connecticut Technology Council Vice-Chair; Board of Directors (2011 – current); Chair of Cyber Security Committee (2013 – current)
Community Action Award (Volunteer of the Year), Connecticut Technology Council, December 2013.
Blue Ribbon Panel member for Criminal Justice curriculum, University of Saint Joseph (current).
Former Member, Audit Committee of the Board of Directors, New York City Housing Authority.
Finalist, Women of Innovation.
Outstanding Contribution Award, Fairfield County American Heart Association.
Outstanding Service Award, Fairfield County Cub Scouts.

Selected as national delegate to National Science Foundation special conference on the Role of Community Colleges in Cyber Security Education.
Committee member, Norwalk Community College, information security curriculum committee.
Chosen as national best practices committee member, Disaster Recovery Institute, Business Impact Analysis.
Chosen as national best practices committee member, Disaster Recovery Institute, Recovery Strategy.
President, Independent Computer Consultants, Fairfield/Westchester.
Outstanding Speaker Award, College and University Machine Records Conference.

Selected Publications/Presentations

Cyber Risk in Captive Insurance Organizations, 2014
Information Security Governance, Eastern European National Information Security Conference, Czech Republic, Keynote Speaker on information security governance and program maturity, 2013
Guest Lecturer on Information Security, Risk, and Governance: Boston University MBA Program, 2010
"HIPAA and HITECH Rules, The New World," presentation and webinar, Stamford, CT, October 2009
"HITECH and Information Security" webinar, International Association of Outsourcing Professionals, July 2009
"Information Security in the American Recovery and Reinvestment Act and HITECH" presentation, May 2009
"Outsourcing in Today's New Risk Averse Climate," October 2008
"Information Security in the Power Industry" webinar, Large Public Power Utility Council, July 2007
"Power Industry Concerns" webinar to Chief Information Officers of major power producers in the U.S., July 2007
"Recovery and Security," International Association of Outsourcers Conference, February 2006
Curriculum Advisory Committee, Norwalk Community College, 2003-2006
Keynote address, Information Security Conference, Norwalk Community College, April 2005
"Information Security Before 9/11 and After," multiple presentations, 2002, 2003
"Securing Web Based Transactions," E-Gov Conference, Tysons Corner, Virginia, March 2001
"Security Weaknesses in the Power Industry," White Paper, October 2000
"Security Needs for E-Business," American Public Power Association, Phoenix, October 2000
"What Penetration Studies Will Teach You," ISACA, Orlando, Florida, July 2000
"Penetration Testing - Why Executives Just Don't Get It," CA-World, New Orleans, July 1999
"Millennium Mayhem," Disaster Recovery Journal, August 1998
"The Realities of Conducting a Business Impact Analysis," IBM Business Recovery Summit, San Francisco, May 1998
"Penetration Testing - Why Executives Just Don't Get It," CA-World, New Orleans, May 1998
"The Realities of Conducting a Business Impact Analysis," Disaster Recovery Institute, Atlanta, September 1997
"Security Review of Netview," Internal Auditing Alert, June 1997

	"Why computer System Penetration Tests Are Needed," Internal Auditing Alert, January 1997 "How to Conduct A Business Impact Analysis," Disaster Recovery Journal, Summer 1996 "Securing MVS," Chapter of Securing Client/Server Networks, McGraw-Hill, 1996 "How to Sell Security to Management," Computer Security Institute, November 1995 "Operating System Controls," Chapter of the Security Manager's Handbook, Auerbach Publishers, 1993 "Security and Controls Will Improve the Bottom Line," Security Management, May 1992 "Controlling Access: A Tiger-Team Approach," Crisis Magazine, January - February 1992 "Information Security in a Short-term Focused World," Crisis Magazine, January - February, 1991 **Selected Interviews/Appearances** Regional News Network (RNN): Richard French Live, panel discussion regarding NSA Ruling, December 18, 2013 Radio Free Europe, "Viruses – Why People Write Them," January 30, 2004 Information Architect Newsletter, "Mainframe Connectivity to the Internet," February 4, 2002 WFDD Radio, "Cyber-terrorism," January 29, 2002 "Security & Business Continuity Since 9/11," Connecticut Bar Association, November 2001 ABC Radio, "Terrorism," September 11, 2001 Many other interviews and appearances, May 1995 - July 2001, details provided upon request.

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

Compliance Auditing

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

Physical Security

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

Appendix B – Tools

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

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

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

[Redacted]

Network Mapping Tools

[Redacted]

[Redacted]

Password Crackers

[Redacted]

System Tools

[Redacted]

[Redacted]

Vulnerability Scanners

[Redacted]

Web Server/Web Application Tools

[Redacted]

[Redacted]

Wireless Testing

[Redacted]

OWASP

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

Attack	Tool
• Un-validated Input	[Redacted]
• Broken Access Control	
• Broken Authentication and Session Management	
• Cross-site Scripting (XSS) Flaws	
• Protocol Analysis	
• Buffer Overflows	
• Injection Flaws	
• Improper Error Handling	
• Insecure Storage	
• Insecure Configuration Management	
• Physical Intrusion	
• IP half-scan	
• Brute Force Password cracking and access violation	
• Cisco devices with SNMP	[Redacted]
• Trojan horses	
• Java-based DB analysis	
• Interceptions; most frequently associated with TCP/IP stealing and interceptions that often employ additional mechanisms to compromise operation of attacked systems (man-in-the-middle attacks)	
• Spoofing (deliberately misleading by impersonating or masquerading the host identity by placing forged data in the cache of the named server i.e. DNS spoofing)	
• Scanning ports and services, including ICMP scanning (Ping), UDP, TCP Stealth Scanning (TCP that takes advantage of a partial TCP connection establishment protocol)	
• Remote OS Fingerprinting, for example by testing typical responses on specific packets, addresses of open ports, standard application responses (banner checks), IP stack parameters etc.	
• Network packet listening (a passive attack that is difficult to detect but sometimes possible)	
• Authority abuse; a kind of internal attack, for example, suspicious access of authorized users having odd attributes (at unexpected times, coming from unexpected addresses)	[Redacted]

• Flooding (Ping flood, mail flood, HTTP flood)	
• Malformed URL's	[Redacted]
• Wireless Connection Attempts	

Appendix C – Sample Deliverables

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

Appendix D – Client Comments

State of Minnesota

[Redacted]

Maryland State Retirement Agency

[Redacted]

Wyoming Department of Health

[Redacted]