



Federal Government uses Backbone Security to conduct Certification and Accreditation

EXECUTIVE BRIEF

- Goal:** To help a department of the Federal Government to meet the GAO requirements in computer and network security. Over 400 systems, worldwide, had to be certified and accredited.
- Solution:** Backbone Security analyzed the situation and rapidly developed a gap analysis and roadmap to correct any deficiencies. Then Backbone set out to improve on what existed and create what was missing to guarantee a passing score on the next government review. Scores of security plans, users guides, procedures and disaster recovery plans were drafted and implemented in a remarkable 24 months.
- Results:** A projected cumulative two-year net benefit of \$7,829,210 was realized through the avoidance of costly in-house resources as well as avoiding internal fines for non-compliance.

A 30% annual ROI was achieved through the process of out-sourcing this manpower intensive operation.

A follow-up audit resulted in the department moving from a failing evaluation to a successful one and having the framework in place to sustain a passing score for years to come.

A large department of the United States Government with locations in almost every country of the world had a General Accounting Office (GAO) requirement to certify and accredit all of their networked computer systems worldwide. The Government contracting office through the GSA contracted with an 8a firm, TNG, to fulfill this contract. Since the project was large for this small firm, they teamed with Backbone Security to accomplish this task. In 24-months, TNG and Backbone successfully completed 400+ systems. Backbone Security delivered:

- Program Assessments,**
- Risk Assessment Reports,**
- System Security Plans,**
- Contingency Plans,**
- Disaster Recovery Plans,**
- Trusted Facility Manuals (TFM),**
- Security Features User's Guides (SFUG),**
- Standard Operating Procedures (SOP),**
- Configuration Management Plans,**
- Interconnection Agreements,**
- Memoranda of Understanding,**
- Privacy Impact Assessments,**
- Security Test and Evaluation Plans,**
- Security Test and Evaluation Reports, and**
- Security Controls Compliance Matrixes.**

NOTE: This case study was authored by Backbone Security.Com. Results shown are not a guarantee of equivalent performance

Benefits

Objective	Benefits Achieved
Assess the security posture and determine a course of action for remediation.	Backbone Security quickly collected critical information, documents and policies that enabled our analysts to perform a gap analysis and then establish a roadmap to modify and improve existing policies and procedures, write new procedures and develop contingency plans.
Write the critical IT policies and procedures	Backbone employees wrote over 4 million pages of policies and procedures to cover the 400+ systems in locations around the world. The government customer was able to effectively configure and operate their systems securely by following the detailed instructions in these documents.
Test and evaluate the systems after remediation was complete	Backbone delivered the ultimate benefit in the form of a Security Test and Evaluation, where the actual tactics, techniques and procedures were tested and evaluated. The GAO independently verified through an audit that this agency improved from a failing report two years prior to a passing report now.

"Backbone Security really delivered. We originally scoped this project as a three-year endeavor. Our mandate changed to complete it in two years. They were able to meet our request and accelerate the completion by a full 12 months. We were able to complete the task on-time, within budget and in a very professional manner."

Chief Information Officer



The Challenge: Perform over 400 Security Certification and Accreditations in 24-months

Federal Systems must certify that every application has the appropriate safeguards in place and the data processed is secure. The requirement to certify and accredit a system to process data is contained in the Automated Information Systems Security Program Handbook. The requirement is also contained in the Office of Management and Budget Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources. Certification and accreditation provides a form of quality control, it forces managers and technical staff to find the best fit for security, given technical constraints, operational constraints, and mission requirements.

The Federal Government requires all systems that access data to be certified and accredited. For new application systems, the certification process must begin during the design and development stage. Each system must be recertified at least once every three years or if the systems undergo a significant modification or is violated. The minimum, security controls that must be in place include

<ul style="list-style-type: none"> • security plan developed and updated • risk assessment conducted • contingency plan developed and tested • system meets all applicable federal laws, regulations, policies, and standards • in-place and planned security safeguards appear to be adequate and appropriate 	<ul style="list-style-type: none"> • technical and/or security evaluation complete • security rules provided to users and signed by users • test security specifications • in-place safeguards operating as intended
---	--

The Solution

Backbone Security mobilized its entire compliment of security engineers and organized them into teams that specialized in regions of the world. These teams were responsible to collecting, analyzing, drafting and finalizing all the certification and accreditations in their zone. As the work progressed the smaller zones were completed and those team members were added to the areas still working. This "zone approach" allowed Backbone Security to maximize the effectiveness of its workforce and reduced the original three-year completion estimates by twelve months. The customer was able to review and accept the completed work on a rolling schedule that minimized their workload and they were able to start meeting their regulatory requires months ahead of schedule.

This customer separated the Certification from the Accreditation activities. The follow-on contractors depended on clear, crisp and complete Backbone Security deliverables. We received the highest marks and are now being asked to return on additional network security contracts.

The Bottom Line for the Federal Government

An analysis of the implementation shows that the credit union will gain a cumulative two-year net benefit of \$3,648,226, an annual ROI of 30% for the project. The entire project has a payback period of 2 months.

The following chart provides a detailed, two-year analysis.

BUSINESS ANALYSIS OF THE SOLUTION

Project Summary

Annual ROI with Backbone Security Project	30%
Payback Period with Backbone Security (months)	2
Cumulative two year benefit	\$3,648,226
Cumulative two year net cost of Backbone Security's Component of Project	\$2,800,000

Project Costs

	Startup	Year 1	Year 2
Hardware & Maintenance	\$0	\$0	\$0
Software & Services	\$100,000	\$1,200,000	\$1,500,000
Staff Costs for Implementation & Support	\$25,000	\$12,500	\$6,000
TOTAL COST	\$125,000	\$1,212,500	\$1,506,000

Benefits

	Year 1	Year 2
Saving in staff costs @ GS-9 step 6 (\$42,558)	\$1,702,320	\$2,626,440
Saving in staff costs @ GS-11 step 3 (\$47,078)	\$470,780	\$564,936
Compliance to GSA Audit Agency Mandates (cost avoidance)	\$450,000	\$677,250
TOTAL BENEFITS	\$2,623,100	\$3,868,626

Financial Analysis

Net Benefit	(\$125,000)	\$1,410,600	\$2,362,626
Cumulative Net Benefit	(\$125,000)	\$1,285,600	\$3,648,226
Net Present Value	\$7,829,210		
Average Annual ROI	30%		
IRR	1177%		
Payback Period (months)	2		