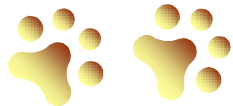
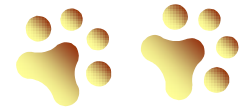

White Paper



A Transitional Approach to Security Certification & Accreditation of Automated Information Systems

By Vernon L. Kirby
Information Assurance Project Director

©2005 NetStar Systems International, Inc.
3702 Pender Drive, Suite 250
Fairfax, VA 22030
703.934.0280 (Telephone)
703.890.0730 (Fax)
www.netstarintl.com



NetStar Systems
International, Inc.

"An 8(a) Woman-owned IT Services Firm"

July 2005

EXECUTIVE SUMMARY

The Federal Government has spent billions of dollars on Information Technology (IT) Security in recent years, but the demonstrated return on investment is less than encouraging. This situation is reflected in a string of Government Accounting Office (GAO) and other reports critical of the general lack of progress at various agencies, and it's highlighted by dismal Federal Information Federal Computer Security Report Card grades that beckon agency Chief Information Officers to the Federal woodshed.

Security certification and accreditation (C&A) of information systems has evolved as the key means of determining the health – and sometimes the financial viability – of Federal IT systems. The C&A process is the current standard for improving the information assurance posture of IT systems; and the process has considerable merit. But current manifestations of the C&A process are generally laborious, cumbersome, costly, create reams of documentation and, most importantly, they don't guarantee secure information systems. The Federal Report Card showings of recent years indicate a sort of Attention Deficit Hyperactivity Disorder on the part of federal agencies: There's a lot of feverish activity, but the result is often counterproductive.

The optimal approach to information assurance (IA) /security requires re-evaluation of the way information security in general, and the C&A Process in particular, is being addressed. The most efficient and effective approach would involve standardization and simplification by creating, supporting – and mandating – a single, general-purpose, tailorable C&A process for all Federal automated information systems. Ideally, this process would be simplified to more directly address security concerns while minimizing complexity and redundancy.

Until that wondrous day arrives, however, the most efficient way to leverage existing C&A processes is to identify and organize all relevant requirements, guidance documents and best practices into electronic libraries. These can be mapped to specific tasks and sub-tasks within the particular C&A process that is being applied. The resulting database can then readily be adapted to any agency-specific requirements and can evolve through the addition of new best practices. Existing Commercial-Off-The-Shelf (COTS) products can be utilized for database management and project management. Administration tools can be employed to reduce expenditures of time and money.

SecurityCAT® – a transitional C&A methodology bridging the gap between today's "As Is" inefficiency and the "To Be" world of tomorrow – has been developed by NetStar Systems International (NSI). SecureCAT® was created following an in-depth assessment of each of the four major C&A processes (NIST, DITSCAP, DCID6/3 and NIACAP).

NSI selected best practices to support each process and developed templates and simplified forms to support major C&A tasks. Using project C&A process models, NSI encapsulated the flow of each required process in a concise, visual manner, avoiding the necessity of reading voluminous instruction manuals. Each step in this process model has associated notes that describe required tasks and direct the user to best practices and templates to create required documents.

The C&A processes are linked to checklists with questions that facilitate rapid assessment of the target AIS's security posture. The tasks in the model are linked to answers provided through completion of the checklist and quickly result in a granular C&A process schedule that provides level-of-effort estimates and/or a project management plan. SecurityCAT® can be used for the management or marketing of C&A services. It also

supports the security documentation developer by guiding the steps that must be followed, the documents that must be completed (in the correct order) and related tasks.

Although there is increasing momentum toward building better security into Automated Information System (AIS) products and processes – and an ongoing effort to provide automated tools and checklists that help to facilitate the information security process – today's demands require us to make better use of the tools that currently are available. Streamlining, consolidating and standardizing existing AIS security C&A processes is something that must be done *now* to reduce complexity, save money and increase the overall security of the nation's information infrastructure. This can be achieved through utilization of NetStar's SecurityCAT® information system C&A toolkit.



TABLE OF CONTENTS

EXECUTIVE SUMMARY	I
INTRODUCTION	1
NEEDED: A PARADIGM SHIFT	2
BEST CASE SCENARIO	3
STANDARDIZE THE PROCESS.....	5
SUPPORT THE PROCESS	6
MEASURING SUCCESS.....	7
BRIDGING THE GAP	8
METHODOLOGY IS NOT ENOUGH.....	8
CONCLUSION.....	9

INTRODUCTION

Although the Federal Government spent approximately \$4.2 billion on Information Technology (IT) Security in FY 2004, most Federal agencies continue to be chronic information assurance underachievers. The grades on the Federal Information Security Management Act (FISMA)-based Computer Security Report Card rose 2.5 points last year – but only to a D+ average.

Security certification and accreditation (C&A) of information systems has become a key measure in determining the status of agencies' information security programs. The C&A process is the current standard for improving information assurance and security. Properly applied, the C&A process goes a long way toward meeting that goal. But the process is cumbersome, time-consuming, expensive, often document-intensive and does not always result in secure information systems. Federal agencies are reporting increasing numbers of information systems certified and accredited, but some agencies still have not certified a significant percentage of their systems.

FEDERAL COMPUTER SECURITY REPORT CARD						February 16, 2005
GOVERNMENTWIDE GRADE 2004: D+						
	2004	2003		2004	2003	
AGENCY FOR INTERNATIONAL DEVELOPMENT*	A+	C-	DEPARTMENT OF STATE	D+	F	
DEPARTMENT OF TRANSPORTATION	A-	D+	DEPARTMENT OF TREASURY**	D+	D	
NUCLEAR REGULATORY COMMISSION	B+	A	DEPARTMENT OF DEFENSE**	D	D	
SOCIAL SECURITY ADMINISTRATION	B	B+	NATIONAL AERONAUTICS AND SPACE ADMINISTRATION	D-	D-	
ENVIRONMENTAL PROTECTION AGENCY	B	C	SMALL BUSINESS ADMINISTRATION	D-	C-	
DEPARTMENT OF LABOR	B-	B	DEPARTMENT OF COMMERCE	F	C-	
DEPARTMENT OF JUSTICE	B-	F	DEPARTMENT OF VETERANS AFFAIRS**	F	C	
GENERAL SERVICES ADMINISTRATION	C+	D	DEPARTMENT OF AGRICULTURE	F	F	
NATIONAL SCIENCE FOUNDATION	C+	A-	DEPARTMENT OF HEALTH AND HUMAN SERVICES	F	F	
DEPARTMENT OF THE INTERIOR	C+	F	DEPARTMENT OF ENERGY	F	F	
DEPARTMENT OF EDUCATION	C	C+	HOUSING AND URBAN DEVELOPMENT	F	F	
OFFICE OF PERSONNEL MANAGEMENT	C-	D-	DEPARTMENT OF HOMELAND SECURITY	F	F	

Figure 1: 2005 Federal Computer Security Report Card

In addition, agency certifications and accreditations do not always meet criteria identified in Federal guidance. Taking stock of the situation, the Government Accounting Office said: “Unless such criteria are met, agencies cannot ensure that accrediting officials are receiving consistent information on which to base their decisions, and the value of this process as a management control for ensuring information system security is limited.”¹

¹ GAO Report Number GAO-04-376, titled “Information Security: Agencies Need to Implement Consistent Processes in Authorizing Systems for Operation,” which was released on July 28, 2004.

While efforts are underway to completely revamp the approach to achieving information security, a specific overall solution continues to be elusive. The purpose of this White Paper is to discuss methodologies designed to streamline and improve the current information system C&A process – to make it more efficient, and therefore more cost-effective – and to improve the overall quality of the products and processes needed to secure the nation’s increasingly interrelated and vital information systems now. This efficiency can be achieved through utilization of the SecurityCAT[®] toolkit developed by NetStar Systems International (NSI).

NEEDED: A PARADIGM SHIFT

The optimal approach to information assurance/ security will require a paradigm shift on the part of the Federal Government and will demand a fresh look at the way information security is being approached. The Federal Report Card showings of recent years indicate a sort of Attention Deficit Hyperactivity Disorder on the part of federal agencies: There are multiple processes and a plethora of activity, but much of it is duplicative, unfocused, wasted or counterproductive effort that results in poor performance aggravated by information overload.

Just as the creation, storage and dissemination of information has evolved over the past several decades from manual to automated means, so too, achievement of secure information systems increasingly involves moving from inefficient manual processes to the application of automation. Vulnerability scans – including use of source code vulnerability scanners that analyze software programs during their development to quantify the level of risk they pose to system operations – will increasingly be applied to streamline the process of addressing threats and vulnerabilities. Automated tools that facilitate other aspects of information security, including C&A documentation, are being marketed and refined.

The optimal Federal Information Systems Information Assurance/Security process is:

- **Simplified**
- **Centralized**
- **Standardized**
- **Repeatable**
- **Fast**
- **Economical**
- **Smooth**
- **Not document-intensive**
- **Automated to the maximum extent possible**

This will result in:

- **Improved, measurable, consistent Government-wide security processes and controls.**
- **Improved, seamless, secure information sharing and interoperability between Government departments and agencies.**
- **A knowledge-base of requirements, manuals, best practices and other guidance.**

But while there are plans to develop an increasingly automated and standardized approach to C&A – and while progress is being made to identify and use common solutions – the need to improve the security posture of the nation’s information infrastructure is immediate and pressing. Current C&A processes can go a long way toward ensuring information system security/information assurance. However, they are inherently labor- and document-intensive and are often being inefficiently applied (if at all), not making full use of a standardized, organized, streamlined, repeatable methodology. The GSA, along with the OMB, recently launched a major effort to identify better methodologies for achieving Federal information security.² But even with an aggressive development engagement, whatever new solution that is identified will be months – or more likely years – away from development, testing, fielding and implementation throughout the huge Federal information architecture.

It is clear that an interim approach is required that combines existing processes, makes fuller use of existing methodologies, and applies best practices to full advantage.

BEST CASE SCENARIO

Under the best case scenario, there would only be one tailorable C&A process for automated information systems that would be applied to all Federal departments, agencies and organizations, including DoD and the Intelligence Community. This single process should be simplified to address security concerns directly and with minimum volume and complexity. The reduction in complexity would eliminate unnecessary and duplicative documents. The process improvement would ensure that boiler plate information is not repeated in every document. Many or most non-automated document output formats could be templates, form-oriented outlines or checklists.

‘Nineteen of the agencies we surveyed ... reported that they had encountered staffing challenges for their certification and accreditation activities that essentially consisted of the need for full-time staff with the appropriate backgrounds, specialized skills, and security clearances. In addition, 13 agencies reported challenges in providing training to staff or officials responsible for certifying or accrediting agency systems.’

—GAO Report 04-376

² GSA Request for Information, #GSV05PD0054– *Information Systems Security*, April 4, 2005.

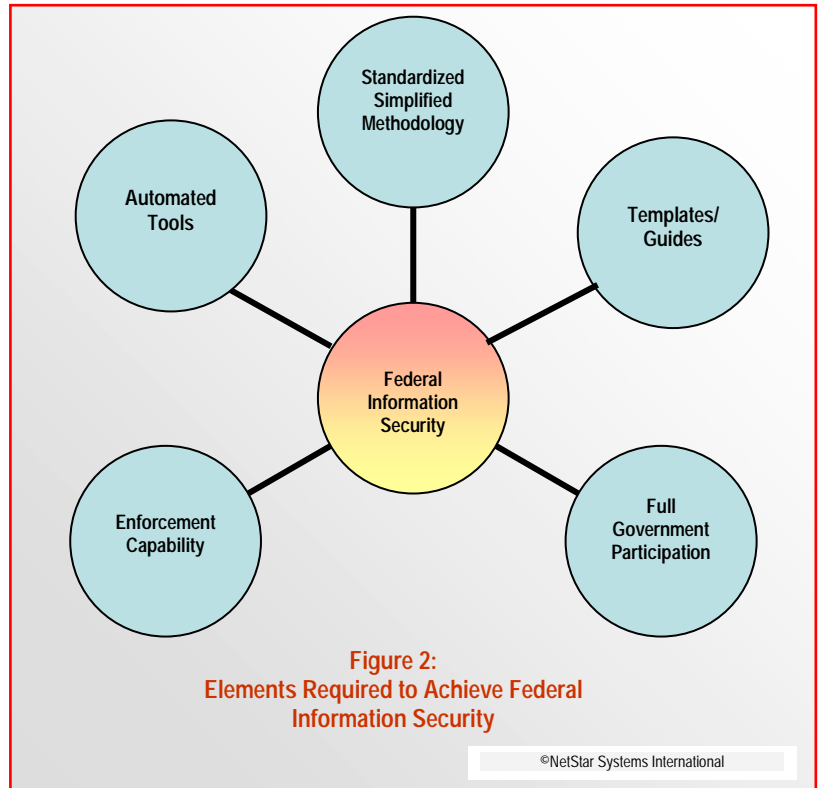
While there are legitimate differences between types of information systems and levels of risk, they all share common characteristics and face a common set of risks. By and large, the development of separate processes, controls and requirements littering the current C&A landscape seems to be based more on a “political” rather than a pragmatic line of reasoning.

Current standards tend to produce encyclopedic documentation that is unnecessary, wasteful, sometimes incomprehensible and frequently counterproductive.

Essential processes, procedures and other information often are buried and obscured by bloviation and unnecessarily arcane terminology. This can impede good security practices and escalate both inefficiency and cost through inordinate consumption of time and other resources required to generate, read, copy, review, revise, maintain current, and store them.

A more efficient approach could be similar to the current Security Plan or System Security Authorization Agreement (SSAA) concept, but the appendices supporting the Security Plan would, to the maximum extent possible, be templates, checklists or form-oriented documents (perhaps automated) that avoid boiler plate and other duplicative information. The C&A process guidance and output documents could be developed using a knowledge-base approach to efficiently convey information to the personnel responsible for system security. The types of approaches described above can be used in all areas of the C&A process. As an example, the standard Risk Management process involves a large amount of documentation that attempts to describe the process and provide guidance. A model, template or checklist approach could produce optimum results while avoiding creation of massive risk management documents.

Another approach that could be used in the risk guidance/assessment area is development of templates of systems with various common characteristics. This approach would quickly focus risk/threat assessment requirements and/or activities. An expert in the risk/threat assessment area would develop a set of parameters (Closed System, Internet, Intranet, Classification Level, Protection Level, etc.) that would characterize systems into different classes. These classes would each have a different risk/threat assessment approach (model or template) and set of



requirements/activities to be completed in the risk/threat assessment area. These class models or templates would address the overall risk requirements and processes required for each class of system. Personnel performing the risk assessment would then do the following:

- (1) Characterize the AIS using the expert system model or template (Closed System, Internet, Intranet, Classification Level, etc.).
- (2) Based on the results of the characterization of the system (use of the expert model or template), the risk assessor would then be directed to a detailed system class model, or template.
- (3) This class model or template would explicitly guide the risk assessor through the risk/threat assessment process for that class of system. In this way, a few knowledge experts (the people who design the characterization questions and the detailed risk class models or templates) would reduce the level of effort of the many contractors and Government personnel who have to conduct the day-to-day risk assessments.

The output documents from the risk/threat assessment process above would not be encyclopedic, but rather could be as simple as a completed template and/or checklist with some short narrative/explanatory information. This concise information could then be incorporated as one of the attachments to the Security Plan/SSAA.

STANDARDIZE THE PROCESS

The Government Information Assurance solution should be backed by amendment to FISMA or by other Congressional Act mandating adoption of the standardized approach across Government. This would ensure implementation of common solution and thereby:

1. Simplify administration.
2. Reduce paperwork/documentation.
3. Leverage C&A data.
4. Simplify adjustments to the process (one adjustment instead of many).
5. Enable Government to focus more resources on perfecting tools/resources rather than feeding process requirements.
6. Maximize training.
7. Greatly reduce duplication of effort.
8. Achieve overall economy of scale.
9. Facilitate application of expertise across Government. (Those trained and experienced in a standardized process can apply their knowledge and experience across the board rather than having to learn a new process if they change agency/position.

Without a strong compliance mechanism, adoption of a common solution is undermined and it is likely that many agencies will continue to flounder.

SUPPORT THE PROCESS

Although the major C&A processes themselves are well thought out and clearly defined (particularly DITSCAP and Director of Central Intelligence Directive [DCID] 6/3), the application of the C&A processes and implementation of a risk-based approach to security controls tends to be rather haphazard and irregular. For instance, development of the DITSCAP SSAA security plan is very clearly described and outlined/templated. However, the appendices that make up the bulk of the overall SSAA are not well defined. Templates and guides are available for some of these documents but not for others. Some agencies have standards for development of these documents; others do not. Sometimes the C&A process is rigorously applied; sometimes not. Some web-based Government IA resource libraries are complete and well organized in requirements sections, but not in those sections that provide access to support material and guidance.

One way to leverage existing C&A processes is to identify and organize into electronic libraries all relevant requirements and guidance documents and best practices that can be applied to each C&A process. These can be mapped to specific tasks and sub-tasks in the particular C&A process that is being applied. Made widely available, the resulting database can readily be adapted to any agency-specific requirements or emergence of new best practices. COTS products can be applied to database management and project administration to enhance efficiency and cut costs. As indicated above, this solution can be supplemented with other automated tools, as required, but the driver is an assessment and determination of the most efficient way to achieve C&A and FISMA compliance for a particular system.

Cost savings and other benefits can be achieved through implementation of a streamlined approach, as described above, that results in efficient application of existing procedures and higher quality documentation — and that reduces the currently substantial timeline for completion of successful C&A. This solution would enable more consistent, comparable, and repeatable assessments of security controls in DoD and Federal AISs. It also would promote better understanding of agency-related mission risks resulting from the operation of the AIS and create more complete, reliable, and trustworthy information for authorizing officials, thereby facilitating informed security accreditation decisions.

NSI has announced the general availability (GA) of its SecurityCAT[®]. NSI fully expects that utilization of the toolkit will immediately result in a much more efficient, refined and cost-effective C&A process. SecurityCAT[®] has the capability to reduce

'According to OMB's March 2004 report to the Congress, funding for IT security has increased from \$2.7 billion in FY 2002 to \$4.2 billion in FY 2003. Nevertheless, a total of 18 agencies identified funding as a challenge to performing their certifications and accreditations.'
—GAO Report 04-376

C&A project labor by an estimated minimum of 30 percent over a typical C&A engagement while increasing the quality of the Security Plan/SSAA, including all appendices, in a measurable fashion over documents created “from scratch.” By providing best practice templates and guidance for the development of C&A documentation, the NSI approach also improves and streamlines the documentation capability for the client AIS.

By providing best practice templates and guidance for the development of C&A documentation, the NSI approach also improves and streamlines the documentation capability for the client AIS.

SecurityCAT[®] is essentially a program management approach – but a muscular one that goes well beyond mere planning, scheduling and resource allocation. The toolkit allows managers to plan and track each specific task and subtask in the four major C&A processes, including timelines, costs, and resources (personnel). It links each applicable task to a specific guidance document, template or other resource that can be applied to facilitate efficient completion of the task, including

development of required documentation leading to a complete Accreditation Package.

SecurityCAT[®] provides a checklist-driven, project-based approach that quickly identifies an organization’s C&A status, needs and requirements – and then instantly translates those requirements into detailed C&A Tasks and Deliverables, Required Resources (People), Project Costs and an overall C&A Schedule. SecurityCAT[®] can be used throughout the system’s lifecycle to track and address security requirements on an ongoing basis. SecurityCAT[®] enhances the efficiency and cost-effectiveness of implementing any of the “Big Four” C&A processes – DITSCAP, NIST, NIACAP and DCID6/3.

SecurityCAT[®] features reliable functionality and data retention, enhances security team efficiency, cohesion and flexibility and includes the capability to maintain Security Plan document version control. By facilitating the C&A processes, including development of Security Plans/ System Security Authorization Agreements (SSAAs) and related documentation, the NSI SecurityCAT[®] provides the capability to meet the situational awareness requirements specifications described above.

MEASURING SUCCESS

Detailed milestone cost and timeline projections built into this COTS-based approach support achievement of successful C&A (approval to operate) of the information system on time and on budget.

The overall project is managed using software adapted to each C&A process and tailored to each specific project. Risks can be tracked and managed through development of a project risk management plan of action and milestones (POA&M)

that thoroughly identifies all risks and identifies resources and strategies to resolve issues. Best Practices for each C&A process can be organized, updated, standardized (where possible) and made widely available. Tools and training are made available covering all aspects of security plan development and implementation.

BRIDGING THE GAP

The transitional C&A methodology bridging the gap between today's "As Is" inefficiency and the "To Be" world of tomorrow was developed after an in-depth assessment of each of the four major C&A processes (NIST, DITSCAP, DCID6/3 and NIACAP), selection of best practices to support each process and providing templates and simplified forms, whenever possible. This approach, using project C&A process models, captures the flow of each required C&A process step for all the major C&A methodologies. This approach also captures each C&A process in a concise, visual manner, thereby avoiding the necessity of reading a voluminous instruction manual. Each step in this C&A process model has associated notes that describe what has to be done for that step and that also describe and direct the user to best practices and templates to create the documents required for that step.

These C&A processes are linked to checklists with questions designed to quickly assess an AIS's security posture. The tasks in the model are linked to the answers provided through completion of the checklist and result in a detailed C&A process schedule that can be generated within a few hours and provide level-of-effort estimates and/or a management plan for the C&A project. This C&A process model also contains estimated resources required and estimated duration times for each process step. Thus, the tool can be used for management, marketing and as a guide for the security documentation developer, guiding the steps that must be followed, the documents that must be completed (in the correct order) and related tasks.

The model adds into the overall C&A process flow the required documents that must be developed. The major C&A process flows currently lack explicit guidance about which documents must be developed and at which stage in the process they should be completed. The interim C&A process model adds these capabilities. In addition, by using embedded notes, the C&A process model can be evolved into a training tool for AIS personnel who will be implementing any of the major C&A processes.

METHODOLOGY IS NOT ENOUGH

It cannot be overemphasized that, by themselves, no set of requirements or standardized procedures – and no toolkits that facilitate compliance – will result in an automated information system that ensures information confidentiality, availability, integrity, authentication and non-repudiation. There also must be full participation in the process by all parties involved in order for it to succeed. This is

clearly delineated in the roles and responsibilities sections of current major process documents, particularly the DITSCAP Manual and NIST 800-37 *Guide for the Security Certification and Accreditation of Federal Information Systems*. However, many CIOs, Program Managers and others in charge of Federal and DoD automated information systems seem to have little understanding of – and commitment to – the level of effort (especially including Government personnel) required to achieve successful C&A and hence ensure the security of the systems for which they are responsible. This is reflected in the very poor showings of most Federal agencies in the annual FISMA-based Federal Computer Security Report Card cited above.

Beyond the application of tools and processes, appropriate administrative controls need to be in place in order to successfully complete a C&A effort and achieve information security. The C&A process, including all products and services, needs to be clearly defined in all relevant statements of work in order to provide a firm foundation on which to build the C&A structure for the information system. This is a relatively simple but critical administrative step to successful, efficient completion of the C&A project. Development and wide distribution of a template C&A SOW or simple guidance document should be considered. Program Managers or other Government officials responsible for fielding the AIS need to thoroughly understand the C&A process (at a high level) and commit resources to efficiently accomplish successful system accreditation.

Reducing the complexity and time/funding commitment necessary to achieve C&A through a standardized, streamlined approach would encourage fuller participation, increased products quality and a high level of information assurance resulting in a more secure information architecture – and report cards that will make taxpayers a lot happier with the Government's efforts.

CONCLUSION

Information security is an increasing concern for both private and Government organizations. In the information chain, AIS interconnectivity has greatly increased the vulnerability of each system by making it only as secure as its weakest link. The various C&A processes are a moderately successful attempt to monitor security and patch up holes as they are identified, but these processes are enormously complex, hugely expensive to implement and wastefully overlapping or duplicative.

Government policy makers and other entities – aided and abetted by eager contractors – are much better at creating and imposing labyrinthine standards and requirements than they are of providing the tools and other resources that must be wielded to meet those requirements. By and large, the Government has ordered a poorly-trained, ill-equipped army of AIS program managers, technocrats and

information specialists to defend the shifting and amorphous borders of the nation's information infrastructure.

Although there is increasing momentum toward building better security into AIS products and processes – and an ongoing effort to provide automated tools and checklists that help to facilitate the overall information security process (including C&A) – there are immediate threats that must be dealt with now. While we must continue to work toward a more automated solution, we also have to engage in a vigorous real-time effort to make better use of the tools that currently are available.

Streamlining, consolidating and standardizing existing AIS security C&A processes is something that must be done *now* to reduce complexity, save money and increase the overall security of the nation's information infrastructure. NetStar Systems International's SecurityCAT[®] has been developed to meet these objectives.

Vernon L. Kirby is an Information Assurance analyst who has supported and managed successful security certification and accreditation (C&A) and re-accreditation of mission-critical Department of Defense automated information systems (AISs). He is co-developer of NetStar Systems International's SecurityCAT[®] toolkit, which includes modules that support and facilitates information assurance and security C&A of automated information systems under the four major Federal C&A processes – DITSCAP, DCID6/3, NIACAP and NIST. Mr. Kirby has developed and maintained Security Plans and System Security Authorization Agreement (SSAA) documentation, including Continuity of Operations Plans, Incident Response Plans, Security Requirements Traceability Matrices, Security Test Plans, Security Policies, Information Assurance Training and Education Plans, and Risk Management Plans. He has participated in security testing and evaluation and contingency/response plan exercises, providing results analysis and reports of findings and recommendations.

