Fielding Simulation and Training Systems Legally Without Accreditation

Mr. Craig D. Thornley
PEO STRI, Cyber Security Office
Orlando, FL
Craig.Thornley@us.army.mil

Mr. James R. Newkirk
PEO STRI, Cyber Security Office
Orlando, FL
James.R.Newkirk@us.army.mil

ABSTRACT

Despite the process improvements resulting from the Department of Defense (DoD) Information Assurance (IA) Certification & Accreditation (C&A) Process (DIACAP), obtaining the required Authorization to Operate (ATO) for simulation and training systems remains a lengthy and taxing chain of events. Though DIACAP has resulted in a more streamlined process and ensures more secure training systems are being fielded to the Warfighter, gridlocks associated with the elevation of validation activities and certification authorities remains a reoccurring encumbrance. In this day of expanding budget cuts, it is imperative to find a solution that achieves the same high level of security while still meeting U.S. and DoD legal requirements with fewer schedule delays and at lower costs.

This paper identifies how this can be accomplished through the utilization of an accredited IA Common Component (IACC). It identifies the fact that IA is still required for all DoD systems and will describe a straightforward process that can easily be adopted in any organization. The paper associates the Platform Information Technology (PIT) classification to training systems and explains the requirements for connecting to other systems, networks or PIT systems outside what is normally considered their accreditation boundary. Most importantly, the paper explains how this can be done without having to go through the formal C&A process.

The PIT system inherits IA controls from the IACC which remains static; therefore, as long as an acceptable risk posture is maintained, modifications can be made to simulation, training and test systems without having to repeat the entire accreditation process. This also relieves the system from annual FISMA and re-accreditation events as well.

This paper convincingly lays out a low-risk approach to fielding state-of-the-art simulation, training and test systems that meet DoD IA requirements in the most efficient manner, allowing the Warfighter to "Train to Fight…Fight to Win" securely.

ABOUT THE AUTHORS

Craig Thornley serves as the Director of the Cyber Security Office and Information Assurance Program Manager (IAPM) for the Program Executive Office for Simulation, Training and Instrumentation (PEO STRI). Craig manages the cyber security program of a $3.5 billion a year organization with over 1100 military, civilian, and industry personnel servicing over 335,000 training systems around the world. He holds many certifications to include the Global Information Assurance Security Leadership Certification (GLSC). He has a Bachelors of Science in Electrical Engineering (BSEE) degree from the University of Central Florida and has specialized training in security engineering and IA. Craig has over 20 years of service to the Government focusing on military intelligence and cyber security.

James Newkirk serves as the Deputy to the Director of the Cyber Security Office in the CIO at the Program Executive Office for Simulation, Training and Instrumentation (PEO STRI) in Orlando, FL. James assists in managing the Cyber Security Office which provides support across the $3.5 billion a year organization with over 1100 military, civilian and industry personnel servicing over 335,000 training systems around the world. James served in the U.S. Navy and then worked as a contractor for the Army before joining the Army Acquisition Corps as a Government employee and has completed over 12 years of recognized Government service. James holds a Bachelors of Science in Business Administration - Management Information Systems (MIS) from the University of Central Florida.

Fielding Simulation and Training Systems Legally Without Accreditation

Mr. Craig D. Thornley
PEO STRI, Cyber Security Office
Orlando, FL
Craig.Thornley@us.army.mil

Mr. James R. Newkirk
PEO STRI, Cyber Security Office
Orlando, FL
James.R.Newkirk@us.army.mil

THE PENDULUM SHIFTS

The process of implementing Information Assurance (IA) requirements and delivering securely configured simulation, training and test systems to the Warfighter has undoubtedly undergone numerous process changes over the years. Gone are the days of complete disregard to IA requirements under the assumption that they will go away with the next swing of the pendulum. The most recent change to the Department of Defense (DoD) methodology for certifying and accrediting systems was the approval of the DoD IA Certification and Accreditation (C&A) Process, commonly referred to as DIACAP. Those that have been through the DIACAP will agree that it has resulted in a more streamlined process compared to previously applied methodologies; however, the elevation of certification activities and accreditation recommendations has plagued the process with burdensome gridlocks along the critical path of obtaining the required Authorization to Operate (ATO).

The concern is, as the number of programs entering the accreditation process increases, the time it takes agencies to process the accreditation packages will continue to worsen. The backlogs at these agencies have grown exponentially and the delays in the process can lead to adverse effects on the critical path of development. Disregarding the requirements however is not a viable alternative and it is clearly stated in such punitive regulations as Army Regulation (AR) 25-2 paragraph 1.5.j, "Military, Federal Civilian & Contractor personnel may be subject to administrative &/or judicial sanctions if they knowingly, willfully, or negligently compromise, damage or place Army information systems at risk by not ensuring implementation of DoD & Army policies & procedures." As the levels of awareness and the amount of policies to protect against the cyber threat increases across the Government, it has become apparent that the next swing of the pendulum will not abolish any of the requirements intended to help protect against those threats.

The question however looms, is there any way to legally develop and field simulation, training and test systems to the Warfighter without having to endure the schedule delays and cost impacts incurred as a result of the accreditation process? The answer is yes! Yes, if the system that is being developed fits the DoD definition of a Platform Information Technology (PIT) computer resource. The PIT systems do NOT have to follow the DIACAP to be Certified & Accredited, nor are they required to conduct annual Federal Information Security Management Act (FISMA) reviews, go through reaccreditation every three years or when a major modification is made to the system. I know – WOW! Can this really be true?

In order to increase training fidelity and better train the Warfighter, more and more PIT systems are being procured with requirements for connecting to other systems and networks, both locally and long-haul. In order to accomplish this however, there are only two ways in which the requirements allow for a connection under these circumstances to take place.

The first option is to undergo C&A of the system utilizing the DIACAP and hope to obtain a favorable accreditation decision in the timeframe that is required for operation. Unless 'hope' is commonly used as a course of action, the second and more preferred method for accomplishing this is to connect the PIT system through an already accredited PIT-Interconnection (PIT-I) or what this paper has identified as the IA Common Component (IACC).

The motivation behind developing this paper was to describe a low-risk approach that can easily be adopted by any organization and how it can properly be executed. Advantages associated with utilizing the accredited IACC for connection will be identified while bringing to the forefront an innovative methodology for complying with DoD requirements and still fielding secure versatile simulation, training and test systems that better allow the Warfighter to "Train to Fight…Fight to Win."

WHAT IS DIACAP

In order to have an appreciation for this approach, it is first important to have a good understanding of the activities which can be avoided when it is not required to go through the DIACAP. Also, it is essential to point out that while some of the C&A activities may be bypassed, this does NOT however mean that the requirements to implement IA into the system can be avoided. By following the process properly, each PIT system still has applicable IA controls implemented and will go through a series of validation activities; however, those activities can be conducted at a lower level than mandated by DIACAP thus reducing the risk of schedule impacts and costs associated with hiring independent certifiers. Whether the system under development is a connected system requiring an ATO, a PIT connected system or even a stand-alone PIT, it is important that IA requirements are identified and included throughout the acquisition, design, development, installation, operation, upgrade and replacement of the system.

It's the Law

The Office of Management and Budget (OMB) Circular A-130 mandates agencies and departments to implement the requirements as defined in Public Law, including the Computer Security Act of 1987 and Title III of the Electronic Government Act of 2002, otherwise referred to as the Federal Information Security Management Act (FISMA). FISMA lays out the framework for C&A, annual Information Technology (IT) security reviews, compliance reporting and remediation planning.

On November 28, 2007, DoD approved DoD Instruction (DoDI) 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP) applicable to DoD information systems with the exception of Sensitive Compartmented Information (SCI) and Special Access Programs (SAP) for intelligence as directed by Executive Order 12333. DIACAP supersedes DoDI 5200.40, DoD 8510.1-M and replaces the DoD Information Technology Security Certification and Accreditation Process (DITSCAP). The establishment of DIACAP was necessary to respond to rapidly evolving changes within IT, influence the way DoD acquires, operates and uses IT and to comply with the emerging Federal requirements and guidelines such as those contained in FISMA. The DIACAP consists of five activities that occur over the course of a system's life-cycle as depicted in Figure 1.

Activity One

The first activity is to 'Initiate and Plan IA C&A.' It is at this stage when the system gets registered and the DIACAP team is first fully assembled at the System Registration Review (SRR). The system's Mission Assurance Category (MAC) and Confidentiality level (CL) are agreed upon at the SRR. This is an important step in the process because the combination of the two establishes which set of DoD 8500.2 IA controls are applicable to the system (further augmented by any Department level controls, i.e. AR 25-2). It is strongly encouraged that the MAC and CL be identified prior to

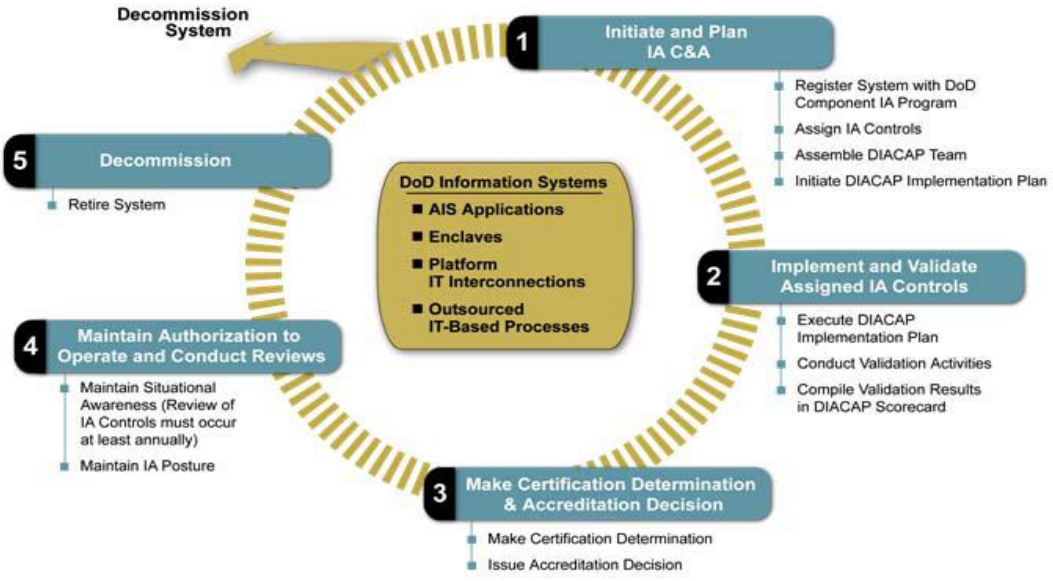

Figure 1. DIACAP Activities

the release of the Request for Proposal (RFP) so that the bidding contractors can propose accordingly. If an RFP is released that does not include the MAC or CL, the question should be posed to the issuing acquisition agency in order to properly scope the IA requirements.

The first activity culminates once the DIACAP Implementation Plan (DIP) is complete and the DIACAP team reconvenes at the DIP Review (DIPR). The DIPR is the final assessment of the assigned IA controls along with their planned strategy for implementation; this includes a review of the implementation status, assigned responsibilities and milestone completion dates for each of the controls. Implementation of the assigned IA controls does impact the design of the system so it is important that the DIPR take place prior to the Critical Design Review (or equivalent). The DIACAP Knowledge Service is an excellent online resource for additional information on the description of IA controls, how to implement them and what their expected test results should be (https://diacap.iaportal.navy.mil).

Activity Two

The second activity is to 'Implement and Validate Assigned IA Controls.' During this activity the agreed upon DIP is executed and validation is conducted by an independent certifier. The certifier must be a vetted Agent of the Certification Authority (ACA). The hiring of an ACA is one of the larger IA related cost drivers impacting a program when having to follow the DIACAP. The costs can vary widely, depending on both the size of the system and the agency selected to conduct the validation. For example, we have seen estimates that range from $40K to over $100K to accomplish the same tasks for similarly sized systems. The results of those validation activities are then analyzed and recorded in the DIACAP scorecard. The System Owner (SO) then prepares a Plan of Action & Milestones (POA&M) which is utilized to identify and track actions required to mitigate any findings discovered during the validation event.

Activity Three

Activity three is, 'Make Certification Determination and Accreditation Decision', which is where the CA reviews all of the DIACAP artifacts and conducts an assessment of the risks posed by the system being accredited and whether or not those risks are acceptable to authorize operation of the system. This has become one of the major schedule risks to a program's critical path due to its occurrence falling late in the development schedule. The reliance on the CA to process the certification determination in a timely manner adds additional risk when there are already substantial backlogs of C&A packages. This is especially difficult when attempting to get a MAC III training system elevated in priority because the MAC level reflects the importance of information relative to the achievement of DoD goals and objectives (MAC I being the highest of importance). It is recommended that a program allow at least 60 days in the program's schedule for this portion of the process.

Once the assessment is complete and a determination has been made, the CA then issues a certification determination to the Designated Accrediting Authority (DAA). The DAA then makes an accreditation decision based on the risk acceptance level they are willing to authorize and the sufficiency of the mitigations in place. The accreditation decision is expressed in one of four levels of authorization:

- Authorization to Operate (ATO) – Valid for a period of three years unless a major change to the system requires a reaccreditation.
- Interim Authorization to Operate (IATO) – Is issued if the system poses an increased level of risk due to unmitigated findings and is issued for a period of 180 days in order to allow time to close out the findings. A one-time extension of 180 days may be issued by the DAA if required.
- Interim Authorization to Test (IATT) – Can be issued to allow short term operation of a system in order to participate in required testing. An IATT is normally issued for a time period not to exceed 90 days.
- Denial Authorization to Operate (DATO) – The DAA may issue a DATO if a system is determined to pose a high level of risk due to the lack of IA controls being implemented. When a DATO is issued, operation of a system must cease immediately and the system must be removed from all networks.

Activity Four

Activity four begins once the accreditation decision is issued and requires the SO to 'Maintain Authorization to Operate and Conduct Reviews.' Once accredited, a system is required to maintain its IA posture through the Information Assurance Vulnerability Management (IAVM) process. Additionally, accredited systems are required to comply with FISMA requirements by conducting the following three annual compliance checks:

- Annual Security Review
- Security Controls Test
- Contingency Plan Test

FISMA compliance is required in order to maintain the system's accreditation properly and will ensure a smoother reaccreditation process which is required every three years. The recurring costs associated with properly maintaining an accreditation are required to be programmed throughout the life-cycle of the system and is the responsibility of the SO. These are costs that can be avoided when a PIT system utilizes the IACC for connection purposes.

Activity Five

Activity five is 'Decommission' which occurs when the system is removed from inventory and operation. Once the decision has been made to retire a system, an assessment must be conducted to ensure there are no impacts as a result of the reliance of inherited IA controls from the retiring system. In addition, documentation needs to be updated and the system must be removed from any registered databases.

WHAT IS A PIT

The DoD Directive 8500.1, Information Assurance, defines a DoD Information System (IS) as a set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display or transmission of information (DoD, 2007, p.16). DoD ISs are categorized in four areas: Automated Information System (AIS) Applications; Enclaves; Outsourced IT-Based Processes and PIT-Interconnections (PIT-I).

An IT component that is not categorized under the DoD IS definition is that of the Platform Information Technology (PIT). PIT refers to computer resources, both hardware and software, that are physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems.

Special purpose systems include but are not limited to a variety of systems such as weapons, training simulators and diagnostic test and maintenance equipment. Therefore, simulation, stimulation, training and test systems that are dedicated to the training or testing of a tactical platform are considered to be special purpose systems and meet the PIT criteria. An example of a PIT system is the AH-64 Apache flight simulator because it is a training system that is dedicated to the mission performance of the AH-64 tactical platform.

PIT & PIT-I IA Requirements

The DoD Information Assurance Directive 8500.1 acknowledges that PIT systems present IA risk management challenges different from those of ISs such as AIS Applications or Enclaves. The underlying premise is that Global Information Grid (GIG) protection is paramount, and thus protection on the platform's IT interconnection to the GIG is the main focus for ensuring security measures are implemented. The PIT itself does have IA requirements, but they can be implemented through the normal system/security engineering design and test regimen without having to comply with the DoDD 8500.1 C&A requirements. PIT systems MUST implement the appropriate level of IA protection that satisfies an acceptable level of risk. If a PIT system is not accredited, its only legal means of connecting to other systems or networks is via a fully DIACAP accredited PIT-I.

As opposed to the PIT, DoD 8500 series policy does apply and is mandatory for the PIT-I. The PIT-I shall utilize pre-determined IA control profiles based on the assigned MAC and CL. These profiles are connection-relevant subsets of the full control sets applied to other DoD information system types, and are subject to the DIACAP process. Again, further details of the profiles are provided in detail on the DIACAP Knowledge Service website (https://diacap.iaportal.navy.mil).

The checklist on the following page in Table 1 can be used to assess the characteristics of systems or components to determine if the IT system meets the PIT criteria. Simply answer the questions in the order provided and depending on the response for each, follow the appropriate action.

INFORMATION ASSURANCE COMMON COMPONENT

To reemphasize, a PIT system does not have to be certified and accredited in accordance with the DIACAP, but if required to connect outside its boundary, it can only do so via an accredited PIT-I. Understanding this, it does not make sense for the developer of every PIT system to have to go through the process of determining what products meet their connection requirements, selecting that product and then having to get that product certified and accredited for operational use.

Table 1. PIT Determination Checklist

Question	Responses	If one or more checked	If none checked
(1) Does the system or component do any of the following with respect to DoD information?	☐ Receive ☐ Transmit ☐ Process ☐ Store ☐ Display	Continue with Question 2 ⇨ Further assessment is required. NOTE: The system/component is required to incorporate IA.	**STOP** **The system/component is not required to incorporate IA and is not subject to the C&A process.**
(2) Which of the following describe the system or component?	☐ It is **physically part of or embedded** in the platform ☐ Its special-purpose mission is **dedicated to** the platform's mission ☐ Its special-purpose mission is **essential in real time** to the platform's mission	Continue with Question 3 ⇨ Further assessment is required.	**STOP** **The system/component is not a Platform IT** and is subject to the C&A process.
(3) Does the mission of the system or component include **general services**, such as e-mail, networking for one or more non- Platform IT systems or business functions?	☐ Yes	**STOP** **The system/component is not a Platform IT** and is subject to the C&A process.	Continue with Question 4 ⇨ Further assessment is required.
(4) Does the system or component perform any of these **special-purpose missions?**	☐ Weapon System ☐ Training Simulation ☐ Diagnostic Testing and/or Maintenance ☐ Calibration ☐ Research and Development (R&D) of Weapon Systems ☐ Fire control and targeting; missile; gun; torpedo; active EW; decoy; launcher; tank; vehicle; artillery; man- deployable system; flight, bridge, classroom training simulator; test or calibration equipment; RDT&E; medical imaging or monitoring; transportation; building;utilities; SCADA ☐ Sensor (acoustic, passive EW, ISR, national, navigational, control); radar; P2P or LOS data link; voice comm.; IFF; C2 of forces; navigation system; GPS; WSN; displays/consoles; tactical support database or decision aid; some portable PCs	**STOP** **The system/component is considered to be Platform IT** and is exempt from the C&A process, but still must incorporate IA. The **System Registration Review (SRR)** must be conducted. The minutes of the SRR will document the system/component PIT determination.	**STOP** **The system/component does not appear to be Platform IT** and is subject to the C&A process.

The IACC Concept

This brings to question, why not develop, accredit and field a PIT-I that acts as a common component which can be utilized for connecting across multiple Live, Virtual, Constructive and Test domains or even a combination thereof? By doing so, the PIT system can inherit the network protection controls from the PIT-I and is relieved of having to undergo the burdensome C&A activities. This is the concept behind the development of the IA Common Component (IACC). The benefits of implementing such an approach are extensive.

The IACC Benefits

As described, the PIT system would be relieved of having to conduct laborious C&A activities under the

DIACAP as well as the annual FISMA testing and reaccreditation maintenance requirements. All of which lead to significant upfront cost savings and more importantly continuous cost savings that occur over the course of the system's life-cycle.

Extracting the IA connection controls from the PIT system and placing them within the IACC relieves the PIT system from having to duplicate those controls and in doing so helps to reduce program costs. This also allows for additional space within the system to be utilized by components that may enhance the functionality of the system.

The IACC baseline remains relatively static throughout its life-cycle. Therefore, once the DIACAP-based C&A is performed on the IACC, the only modifications made to the baseline result from patch management and minor changes made to the configuration settings in order to operate properly. Under the DIACAP, these types of changes are allowed and do not affect the accreditation when implemented in accordance with documented polices of the Configuration Control Board (CCB).

Since the PIT system does not go through the DIACAP, modifications can be made to it that otherwise might have an impact on its accreditation and possibly lead to a reaccreditation. Being able to make these modifications easier, adds to the versatility of the system, allowing it to keep up with the constant changing requirements of the Warfighter and also helps contribute to enhancing the testing and training performed by the system.

Market Research Conducted

It was intended that the IACC functionality would be represented by a product or line of products enabling rapid, secure interconnections to be made between simulation, training and test (PIT) systems with minimal effort. Through market research and a thorough analysis of alternatives, the IACC functionality was found to be met by existing Commercial Off-The-Shelf (COTS) technology.

A single product emerged from the results of the analysis that best demonstrated the capability and functionally requirements that were developed. The primary focus was on that of the Virtual training environment; however the requirements to connect in the Live, Constructive and Test domains were also considerations during the analysis.

The recommended product was chosen based on a methodology that invoked decisions based on evaluation criteria and weighting of those criteria (Mandatory, Desired, High, Medium and Low) in order to objectively identify a product to function as the IACC. During this process, eighteen prospective products underwent evaluation by conducting research of product information and performing trade-off analysis of potential candidates against the evaluation criteria. Finally, a suitable solution based on capability and price was recommended. The product best representing those objectives and functionality requirements chosen to perform as our IACC was the Fortigate® 310B by Fortinet®.

It is important to note that both authors of this paper are Government Civilians and are in no way affiliated with the Fortinet company. Our selection of the Fortinet product does not in any way act as an endorsement for it or any of their products, it is merely the product chosen to act as our IACC based on pre-defined evaluation criteria as described. Other organizations may select differing products to represent their choice for an IACC based on requirements.

Unified Threat Management

The 310B is what is referred to as a multilayered Unified Threat Management (UTM) security device. The UTM refers to products that are comprehensive security solutions which have recently emerged within the network security industry. In theory, it is the evolution of the traditional firewall into an all-inclusive security product that has the ability to perform multiple security functions in one single appliance: network firewalling, network intrusion prevention, gateway antivirus (AV), gateway anti-spam, Virtual Private Network (VPN), content filtering, encryption, load balancing and on-appliance reporting.

Advantages of the UTM

The main advantages of UTM solutions are simplicity, streamlined installation and the ease of patch management due to the ability to update all of the security functions or programs concurrently. So, not only does it result in a more cost-effective purchase, but also day-to-day network operating costs are also lowered considerably. The ultimate goal of the UTM is to provide a comprehensive set of security features in a single product that is managed through a single console.

A single UTM appliance makes it very easy to manage the security posture, with just one device to configure, one source of support and a single way to maintain

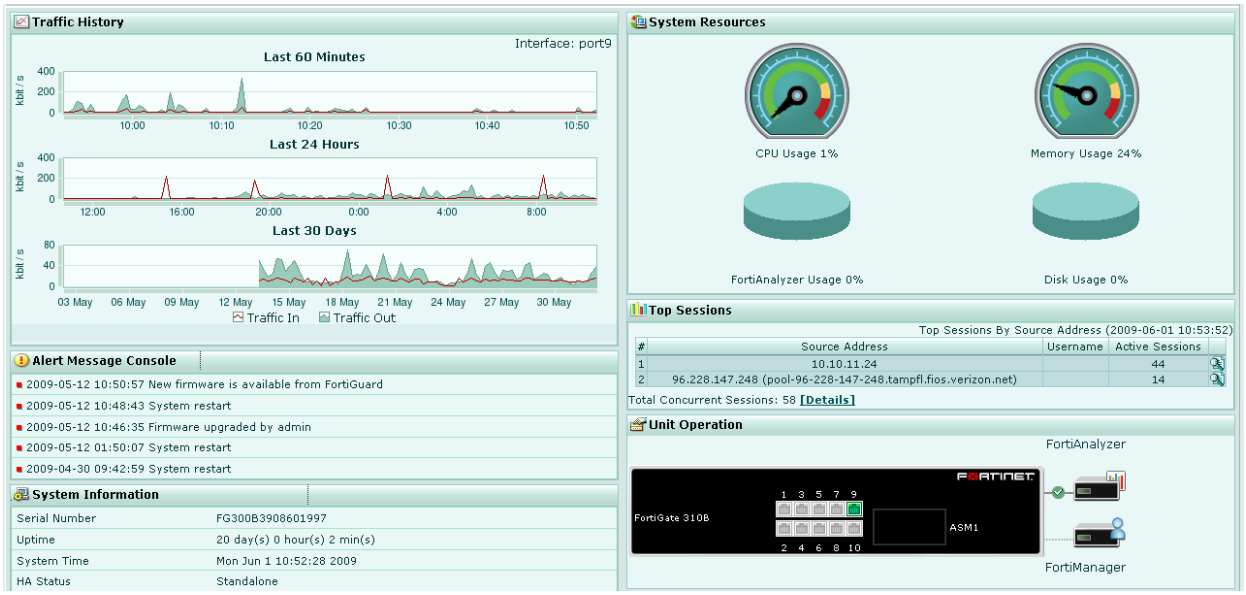

Figure 2. System Dashboard

every aspect of your security solution. The UTM can prove to be more effective of a solution as its strength lies in the bundle of solutions which are integrated and designed to work together. Also, from one single centralized console, all of the security solutions can be monitored and configured in real-time.

The Fortigate 310B's multi-layered security solutions efficiently and economically provides an integrated set of security services in a single, easy-to-manage high-performance appliance that is capable of supporting a wide range of deployment scenarios. The screenshot of the system dashboard in Figure 2 is an example of the user-friendly application that is used for configuring and monitoring operation of the 310B. In addition, FortiGuard™ Subscription Services include everything from technical support, antivirus updates, antispyware, antispam, and Web content filtering to ensure that the security environment remains current and DoD ISs are protected against the latest blended threats.

Potential Drawback

The biggest disadvantage of the UTM lies in the fact that in a complex array of security solutions, the UTM scales back the concept of defense in depth that can lead to a single point of failure. The failure caused by having just one security solution can lead to the entire system being brought down. The mitigation to this risk however is that many PIT systems are not really enclave type systems that operate at the demarcation point between a WAN/LAN scenario. If the system is going to be operating behind an Installation Campus Area Network (ICAN) service provider, then you already have several layers in place protecting the system. Secondly, the 310B and almost all Firewall/IPS/IDS UTM systems default to the "Fail Secure/Safe" mode. So, even if the device were to fail, it wouldn't leave the system vulnerable to attack.

This scaled back concept of defense in depth is allowed when the integrated device is a National Information Assurance Partnership (NIAP) approved product. The DoD Network Infrastructure Security Implementation Guide (STIG) states, "An integrated solution implemented within DoD should not waive from defense in depth practices. Router and firewall integration approved by NIAP is an acceptable solution."

The 310B began the formal process of undergoing the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) evaluation in March of 2006. Products on the evaluation list can be used unless they are removed due to unsuccessful completion of the evaluation; the current estimate for evaluation completion is December 2009. The product is also undergoing Army Technical Integration Center (TIC) testing in order to receive approval for being placed on the Army's IA Approved Products List (AIAAPL).

Finally, most training systems are categorized as MAC III systems in which the consequences of integrity loss or availability can be tolerated or overcome without a significant impact on mission effectiveness or operational readiness. Consequently, a short term failure should not result in any substantial setbacks.

IACC AS THE SOLUTION

Clearly, the advantages of deploying an IACC as the PIT-I solution far outweigh the disadvantages. Sure, even if the system is determined to be a PIT, the option is still there to follow the five activities of DIACAP and pay for an independent certifier to validate the IA controls of the system. Then wait patiently once the recommendation has been submitted to the CA while the accreditation package is processed, finally resulting in the ATO decision being submitted to the DAA. Of course that will then require the annual events associated with DIACAP activity four to be conducted in order to maintain the ATO. All of these events then circulate over the life of the system including a reaccreditation any time a major modification is made or three years has elapsed. These all lead to increased life-cycle costs, schedule delays and impacts to the system's operational availability (A_o).

The recommended solution however is to utilize an already accredited multilayered security interface device such as the IACC. Though the IA requirements do not go away for your PIT system, they will be greatly reduced and streamlined resulting in many advantages from not having to comply with C&A requirements. The greatest of these advantages come from the cost and schedule savings as a result of being able to avoid those requirements and the increased functionality of the system that can come from being able make modifications without affecting its accreditation status. The use of an IACC for connection may not always be the most effective for your program, but the advantages of fielding simulation and training systems without accreditation utilizing this methodology are clear, compelling and most importantly, legal!

ACKNOWLEDGEMENTS

We would like to thank all of the individuals who have contributed to the successful development of the IACC and helping to make the idea a reality!

REFERENCES

Department of Defense, (2007). *8500.01E Information Assurance (IA).*

Department of Defense, (2003). *8500.2 Information Assurance (IA) Implementation*.

Department of Defense, (2007). *8510.01 Department of Defense Information Assurance Certification and Accreditation Process (DIACAP)*.

Department of Defense, (2007). *Network Infrastructure Security Technical Implementation Guide.*

Department of the Army, (2007). *25-2 Information Assurance.*

Department of Defense, (2009). *DIACAP Knowledge Service*. Retrieved June 03, 2009 from https://diacap.iaportal.navy.mil.

Program Executive Office for Simulation, Training and Instrumentation (PEO STRI), (2008). *Basic Accreditation Manual (BAM).*

Newkirk, J. & Piatek, M. (2008). *DIACAP – Information Assurance, Evolved.*