



Mission: Possible

SECURITY TO THE EDGE





Linton Wells II



LtGen Robert M. Shea, USMC

security to the edge

Net-centricity is critical to transformation, and a secured Global Information Grid (GIG) is the cornerstone of this process. To achieve security to the edge and make Joint Vision 2020 and full spectrum dominance a reality, it will require dedication and commitment by all. Information Assurance provides warfighters, commanders, and users the confidence and trust they demand.

Asymmetric threats are real and the results of insecurity are potentially catastrophic. We must protect our information from threats: enemy, criminal, insider, or self-inflicted accidental events that weaken our security. Our information base and our ability to leverage the technology to support warfighting, intelligence, and business functions must have the highest level of trust and confidence or we lose the advantage that information provides us.

The protection of the GIG is everyone's business—this cannot be overstated. We take specific actions to train, license, qualify, and certify pilots and weapons systems users—we must consider no less of a standard for the operation, security, and integrity of the GIG. "Fighting the Net" is the commanders' business, and protecting the net is everyone's business.

This collaborative effort between the CIO and warfighting community is critical. We recognize the importance of the GIG, and we urge everyone to become engaged. The GIG is quickly becoming a Center of Gravity. We need your support to ensure that it does not become our Achilles Heel.

Linton Wells II
Acting, Assistant Secretary
of Defense (Networks and
Information Integration)

Robert M. Shea
Lieutenant General, USMC
Director for Command, Control
Communications and Computer
Systems, The Joint Staff



Trusted information is the key to modern warfighting

Our joint/coalition forces and warfighters depend on trusted information to achieve mission success, protect critical resources, and safeguard the lives of Soldiers, Sailors, Airmen, Marines, and supporting Civilians. Every phase—from planning, arming, and deployment to the coordination of operations with coalition partners around the world—hinges on the availability of reliable, uncompromised information, intelligence, continuity of reach back, and business processes.

At a time when our country's armed services are leveraging the Information Age, availability of a secured, net-centric information environment has become essential. This capability is on its way to becoming a Center of Gravity and the linchpin of our military's transformational approach to net-centric operations and warfare.

Achieving security to the edge to protect sensitive information will require a viable campaign plan—and strong Information Assurance (IA) is central to this plan.

Transformational capabilities covered in the Joint Operations Concept, as well as the transformational goals developed by the Secretary of Defense, support the National Security Strategy and National Military Strategy by emphasizing information superiority as a means of achieving full spectrum dominance. The Department of Defense's (DoD) Joint Vision 2020 defines this as "the ability of U.S. forces, operating alone or with allies, to defeat any adversary and control any situation across the range of military operations."

Joint warfighter requirements must support interoperability between multiple combatants; a mature

the
key



The GIG is a secure grid providing seamless, end-to-end capabilities to all warfighting, national security, and support users.

sustaining base and forward deployed locations; U.S. operations and allied/coalition capabilities; and individual government agencies. There is also a need for capability-based products to produce full spectrum dominance while incorporating robust IA to protect against cyberwarfare attacks.

DoD's emerging Global Information Grid—known as the GIG—is the platform to disseminate information and intelligence to leverage weapons systems and business-process functions. Designed to combine the information resources of all branches of our armed services into a secured infrastructure, the GIG's net-centric approach will link desktops, supercomputers, satellites, weaponry, and more to provide support for intelligence,

logistics, and warfighting. It will enhance DoD's capabilities and support interagency national security interests on a global basis, with a "reach to the edge" to provide members of coalition forces, as appropriate, with services and security. Everything we do—operations, intelligence, logistics, plans and orders, sensing and targeting—will ultimately depend on and move through the GIG, with a trust factor that provides assurance to warfighters and enables forces to move quickly, coordinate operations, strike effectively, and minimize risk.

Because of the sensitivity of the information housed on the GIG, the need for a well-thought-out IA plan is critical. Every individual at every level must be committed to protecting the GIG and the information it contains.

the GIG

The Secured Global Information Grid (GIG) Holds the Future of Warfighting

From its beginnings as a series of loosely connected, unrelated networks, the GIG is evolving into a seamless information environment that provides access to warfighting, intelligence, and business-related processes and information in ways that are assured, available, and appropriately managed—a trusted environment.

Warfighters, weapons systems, and other authorized users and processes can access the GIG at any time from anywhere in the world to obtain the information they need to successfully execute their mission. This on-demand access elevates the communications network to an unprecedented level, with importance commensurate with that of a weapons system,



THE GIG IS THE CENTER OF GRAVITY

and transforms warfighting by reshaping deployment timelines, force allocation, logistical support, target acquisition, and command and control. A secured GIG enables our transition from a collect, process, “push” philosophy to an on-demand “pull” capability from anywhere at anytime.

Today’s warfighter depends on technology, and this warfighting technology cannot execute without trusted information. The GIG’s net-centric approach is at the heart of the transformed kill chain.

Everything we do—operations, intelligence, logistics, plans and orders—will ultimately depend on and move through the GIG.



Everyone, regardless of position or rank, must become involved in protecting the GIG and the information that moves through it.

As the GIG evolves and matures, it will continue to:

- **Build** – Make information available through a network on which users know they can depend and trust.
- **Populate** – Add new, dynamic sources of information to use in defeating adversaries.
- **Protect** – Implement new and better ways to eliminate previously exploitable weaknesses.

As it evolves, the GIG will become a more integrated, scalable, fully distributed information environment adaptable through technology, fully secured, and capable of moving information from any source to any destination. It will provide immediate information to its users through intelligent “pull” technology, and be dynamic, adaptive, self-reconfiguring, and robust. The secured GIG will integrate legacy C4ISR systems, and enable full exploitation and integration of sensor

with weapon systems. The secured GIG will be flexible and embrace future technologies. It is the future of our secured information.

The GIG is leading DoD’s transition into the Information Age by laying a foundation for net-centric operations and warfare.

Because of the GIG’s importance and value to the warfighter, it is quickly becoming a Center of Gravity for warfighting. But without vigilant monitoring and an effective IA strategy, the GIG could just as easily become our Achilles Heel. Everyone, regardless of position or rank, must become involved in protecting the GIG and the information that moves through it. Constant vigilance—at a level similar to that involved in operational security—is required from each of us to achieve continuous mission success.

Information Assurance (IA) secures and enables the GIG and helps safeguard the warfighter

In simplest terms, the GIG enables trusted information to ride on a secured information environment. A secured, trusted information path enables warfighters to access the information they need on demand and react to emerging situations quickly and with confidence.

With strong IA we can achieve security to the edge, assuring GIG users of:

Trust and confidence in their information at all levels.

Commanders must trust and rely without question on the integrity of the information they use to make decisions—it must be accurate, timely, and available when needed. If the commander is distracted by information—if time must be taken to validate and re-check, or stop to think, ponder, or otherwise “touch” the information before it is used—the advantages of speed and agility are lost. Strong IA will ensure higher levels of reliability, minimize risk, and assure that warfighters can achieve success with confidence.

Interoperability. Net-centric warfare has transformed long-held perceptions of time, speed, and geography. On-demand availability of trusted information lessens the need to mass combat power or logistics, and integrated capabilities allow prudent leveraging of resources, enabling warfighters to achieve success under multiple contingencies with “right-sized” forces and tailored logistics. Although the principles of war still

apply, improved knowledge gives commanders agility, enabling them to streamline efforts and choose from a wider range of options. Strong IA enhances and enables interoperability and helps facilitate operational effectiveness. Additionally, interoperability promotes success with multinational and coalition operations and ensures security is an integrated component—not an afterthought or “bolt-on” application.

Access to the right information at the right time.

From an information access standpoint, the GIG is the equivalent of a superhighway with a direct connection to an array of warehouses packed with vital information. Safeguarded by strong IA, on-demand access can be provided to resources that influence how and with what we fight. On-demand access of tactical information can greatly enhance battle planning and execution.

Conservation of resources. Split-based operations are strengthened and achieved as the GIG’s linkage of battlespace and information enables warfighters to capitalize on opportunities. With strong IA in place, fewer personnel and logistics may have to be forward deployed, easing the logistics challenge and freeing resources for other engagements. With strong IA in place, just-in-time logistics eases the physical transportation challenge and footprint and frees resources for other engagements.

it works

A secured, trusted information chain enables users to access the information they need on demand and react to emerging situations quickly and with confidence.





Strong IA can help prevent hostile and unwarranted attempts to disrupt operations.

Situational awareness. The GIG's built-in sensor netting, data fusion, and information management capabilities improve battlespace awareness and knowledge, helping warfighters reduce risk and lessen the need for guesswork. Strong IA can prevent these capabilities from being compromised. Strong IA can also prevent an adversary from using our information to establish their own battlefield awareness.

Reduced likelihood of risk. Because the GIG's role in net-centric warfare leverages the use of information, manpower and materials requirements are decreased. This results in faster response times, reduced hazards to warfighters, increased combat effectiveness, and lower overall costs. Strong IA can save lives.

24x7 availability. Warfighters can rely on the fact that information and services will be available on

demand whenever they are needed. Strong IA can help prevent hostile and unwarranted attempts to disrupt operations.

Under normal circumstances, IA is transparent and goes unnoticed by most users. With strong IA, commanders are confident in their information because five crucial conditions have been met:

- **Confidentiality** – Information is protected from unauthorized entities or processes.
- **Integrity** – Information is protected from unauthorized modification or destruction.
- **Availability** – Information is timely, with reliable access for authorized users.
- **Authentication** – Measures are in place to verify the legitimacy of information and those claiming to be authorized users.
- **Non-repudiation** – Information can be proven to have originated from the sender of record.

Poor IA Impacts Missions and Potentially Costs Lives

Failure to incorporate IA into operations and systems will impact every information-based decision obtained from the GIG. An absence of strong and effective IA is an invitation for our adversaries to infiltrate the GIG and compromise the information it contains.

Depending on the severity of the violation, a compromised GIG:

- Destroys confidence in information provided for decision-making,

eliminating the GIG's usefulness in net-centric warfare and placing warfighters at increased risk.

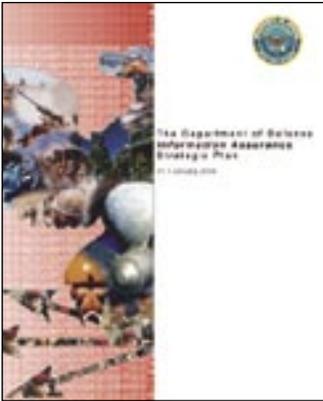
- Produces integration and interoperability issues with coalition partners, disrupting effective coordination.
- Casts doubt on the integrity of core and current systems such as navigational (e.g. Global Positioning System) and situational awareness (e.g. Blue Force Tracking) tools.



- Creates information security issues with authentication, non-repudiation, and related areas.
- Fosters overall doubt and confusion, necessitating a return to non-net-centric methods of warfare.
- Increases time needed for decision cycles and kill chain cycles.
- Affects the concept of operations when increased massing of forces or logistics is required.

With mission success and lives at stake, IA cannot be regarded as an optional add-on...to be truly effective, it must be built into the system at the time of its design. Security to the edge must be maintained to support concepts of operations and ensure the distribution of all required information.

IA cannot be regarded as an optional add-on... to be truly effective, it must be built into the system at the time of its design.



The mission—
to assure DoD's
information,
information systems,
and information
infrastructure.

The IA Strategic Plan lays the foundation for securing the GIG

Protection of the GIG involves five major components: the DoD IA Strategy; Implementation Guidance; the IA Component to the GIG Architecture; Defense-in-Depth support by a robust Joint Staff IA Annex to the C4 Campaign Plan; and Daily Execution and Implementation. These actions will protect the GIG and instill user confidence in the information that moves within it.

DoD's Information Assurance Strategic Plan

The first component is a comprehensive methodology released in January 2004 that directly addresses the GIG's security needs in its five major goals and outlines a number of objectives to support these goals:

Goal 1: Protect information –

Safeguarding data as it is being created, used, modified, stored, moved, and destroyed: at the client, within the enclave, at the enclave boundary, and within the computing environment, to ensure that all information has a level of trust that corresponds with mission needs. This requires:

- Developing and promulgating an IA component to the GIG's IA architecture
- Developing and protecting criteria for net-centric operations
- Developing and deploying protection capabilities across the enterprise
- Applying net-centric operations concepts to the Security Management Infrastructure (SMI)

Goal 2: Defend systems and networks –

Recognizing, reacting to, and responding to threats, vulnerabilities, and deficiencies to ensure that no access is uncontrolled and all systems and networks are capable of self-defense. This involves:

- Establishing a GIG network defense architecture and “to be” baseline
- Developing and enforcing Computer Network Defense (CND) policies
- Evaluating and deploying CND tools and capabilities
- Establishing mechanisms and procedures within CND response action guidelines that effectively utilize CND tools and capabilities to react and respond to events
- Mitigating insider threats

Goal 3: Provide integrated situational awareness/IA command and control (C2) –

Integrating an IA posture into an operational picture synchronized with NetOps and emerging Joint C2 Common Operating Picture (COP) programs to provide decision makers and network operators at all command levels with the tools to conduct IA/CND operations and net-centric warfare. This requires:

- Developing and deploying an Enterprise Sensor Grid (ESG)
- Establishing effective Indications and Warning (I&W) of potential or ongoing attacks against the enterprise
- Developing and deploying an IA User-Defined Operational Picture (UDOP) integrated with evolving NetOps and Joint C2 COP capabilities



- Conducting near-real-time and integrated IA/NetOps decision making across the enterprise
- Harmonizing NetOps, Information Operations (IO), Computer Network Attack (CNA), and CND policies, doctrine, relationships, and operations

Goal 4: Transform and enable IA capabilities – Discovering emerging technologies, experimenting, and refining development, delivery, and deployment processes to improve cycle time, reduce risk exposure, and increase return on investments. This is accomplished by:

- Ensuring that IA is integrated and sustained throughout the life cycle of all DoD programs
- Improving the quality of strategic decision-making

- Expediting the development and delivery of dynamic IA capabilities through innovation
- Enabling efficient information sharing and collaboration across traditional boundaries

Goal 5: Create an IA empowered workforce – Training operators and educating users to equip the workforce to support the changing demands of the IA/IT enterprise by:

- Standardizing baseline IA certifications across the enterprise
- Providing trained/skilled personnel when and where they are needed
- Continuously enhancing IA knowledge and skill levels
- Infusing IA into other disciplines

These goals are the heart of the DoD IA strategy and serve as the foundation for securing the GIG.

The warfighter needs the right information at the precise moment to accomplish the mission.



Achieving the five goals of the IA strategic plan is essential for security to the edge.

two Implementation Guidance

The second component of our plan to enhance IA for the GIG is to develop and implement a suite of DoD IA policies that create the conditions for success. These policies and their implementation guidance must accommodate the dynamic nature of the GIG as it transitions from an enclave-oriented to a service-oriented architecture while maintaining appropriate levels of confidentiality, integrity, and availability. Some of the policies and implementation guidance that move us in that direction are:

DoDD 8500.1 – The overarching IA directive that specifies the high-level policies and responsibilities that will allow the DoD to achieve and maintain appropriate levels of confidentiality, integrity, and availability for all DoD information systems.

DoDI 8500.2 – The implementation guidance for DoDD 8500.1 that establishes a multi-tiered management structure to accommodate evolution of the GIG and provides sets of baseline IA controls that must be consistently applied.

DoDI 8510 – This soon-to-be-published Defense Information Assurance Certification and Accreditation Process (DIACAP) establishes a standard process for identifying, implementing, and validating IA controls; authorizing system operation; and managing the IA posture across all of DoD as we transition to the GIG. This instruction, expected to be released in early 2005, will replace the DITSCAP.

DoDI 8520.2 – Prescribes procedures and assigns responsibilities for implementing DoD Public Key Infrastructure (PKI) and Public Key Enabling (PKE) to achieve a higher level of confidentiality through cryptography, digital signature, and multiple authentication mechanisms.

DoDD 8530.1 and DoDI 8530.2 – These two issuances identify policy, assign responsibilities, and provide procedures essential to support the Commander, USSTRATCOM's CND initiatives.

DoDI 8551.1 – Addresses ports, protocols, and services management at the enterprise level to enhance interoperability and security management of ports and protocols in use.



DoDI 8570.1 – Establishes IA Training, Certification, and Workforce Management requirements and procedures for the entire DoD IA workforce. It also mandates the identification, tagging, and tracking of IA personnel, positions, and certification status.

DoDI 8580.1 – Provides for integration of IA into the Defense Acquisition System by specifying required and recommended levels of IA and prescribing an IA strategy process for the acquisition of mission critical and mission essential systems.

**Protecting the GIG
requires teamwork at
every level.**

CJCSI 6510.01D – This CJCSI on IA and CND contains detailed procedures that complement the guidance issued in DoD 8500 series directives and instructions.

CJCSI 6212.01C – This CJCSI includes Net Ready Key Performance Parameters (NR-KPP) and IA requirements for Joint Capabilities and Integration Development System (JCIDS) interoperability and supportability certification and validation of Information Technology and National Security Systems.

In addition to the above-mentioned directives and instructions, there are a number of other targeted subject and focus areas in which policy and instructions have been issued or are nearing completion.

three Information Assurance Component to the GIG Architecture

A third component of our plan relates to developing standardized architectural concepts for securing and enabling the GIG—building IA into the GIG’s basic framework. The IA Component of the GIG Architecture is an evolving effort that draws on key DoD IA strategies and findings and describes the systems engineering methodology needed to realize DoD’s vision of assured enterprise architectures and achieve interoperability and a security blueprint. The products of this effort are not stand alone but rather a staged IA migration approach that provides content that will be integrated into DoD’s

GIG architectural documents and resource, requirements, and acquisition processes to ensure the integration of coherent IA into GIG programs.

The end state of this architectural process is the transformation from a need-to-know to a need-to-share information protection model, enabled by tightly integrating IA within a net-centric enterprise capability.

The cornerstones of IA for the GIG are:

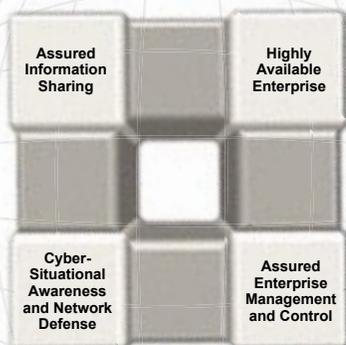
Assured information sharing.

Information and services must be known to be authentic and uncompromised. A balance between need-to-know and need-to-share should be achieved through dynamic access by U.S., allied, and coalition forces to information at multiple classification levels.

Highly available enterprise.

Services must be operational when needed, despite hostile attempts to terminate or disrupt access. Computing capabilities, communications resources, and information services must be available to support net-centric operations. Services should be available to GIG users through the information enterprise, with end-to-end protection of information, prioritized resources, robust connectivity to provide multiple options and routes, and minimal downtime when systems or components fail. Security and availability must reach to the edge of the GIG.

The cornerstones of IA for the GIG.

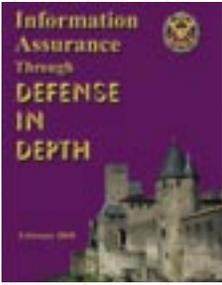




Cyber-situational awareness and network defense. Requires near-real-time awareness of enterprise threats, status, and performance. The ability to respond appropriately, with awareness of external attacks and insider abuse/misuse of GIG resources, is essential. Network defense strategies such as detection, monitoring, analysis, and response must also be in place.

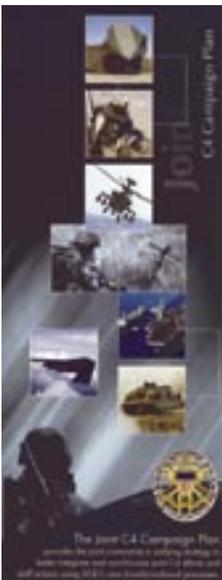
Assured enterprise management and control. The enterprise must operate as intended, with the GIG management and control processes and information protected and a security infrastructure in place. This security infrastructure must support a net-centric environment for large numbers of users and managed assets in a global setting.

IA efforts will provide a standardized baseline for interoperability and serve as a blueprint to be leveraged by future technologies.



Defense-in-Depth describes the integration of people, technology, and operations as the means of safeguarding the computing environment.

Integrated IA priorities match COCOM operational requirements.



four **Defense-in-Depth**

The fourth component of the plan to strengthen security and enhance the GIG includes the evolving components of Defense-in-Depth (DID) and the Joint Staff's IA Annex to the C4 Campaign Plan initiatives that support a robust DID. The DID uses well-known tactical and operational methods to safeguard the computing environment. Earlier versions of the DID were based on securing the perimeter and adding increasing rings of perimeter security to provide added protection for selected important systems and capabilities. As security of the GIG evolves and newer tools become available, we need to evolve our DID strategy. Technology was leveraged, and this transformed the process from a perimeter defense concept to embedding security across the fabric of the enterprise down to and including the data element.

As security moves from the perimeter to interior portions, we achieve defense-in-breadth as well as defense-in-depth. The foundation of people, technology, and operations are as vital today as when the concept of DID arrived on the scene. The transformational shift of security, embedded in the fabric, strengthens the security posture and truly adds depth and breadth to our security posture.

The Joint Staff's IA Annex to the C4 Campaign Plan strengthens the security process by actively pursuing near-term (0–36-month range) solutions. It leverages the five goals of the IA Strategic Plan and synchronizes the joint strategic IA vision to bring workable solutions to the force sooner. The Campaign Plan links capability, focused time line, completion dates, and assigned responsibilities to achieve Defense-in-Depth from the perimeter to the embedded fabric of the GIG.

five **Daily Execution and Implementation**

Creating and maintaining a secured network requires the dedication and commitment of everyone. Our communications networks, including the GIG, are assets whose proper functioning is as critical as that of any weapons system. Just as pilots must be licensed and certified, tank crews are required to conform to pre-determined standards, and naval surface warfare officers must achieve specific levels of proficiency, so should our computer and GIG operators be required to undergo training and certification.



In this sense, IA is similar to operational security—everyone has a role, and each person must come to the realization that his or her participation is vital.

- Resource allocators must be made aware of—and realize the importance of and necessity for—IA
- IA professionals within our armed services must be trained, certified, and tracked through subsequent duty assignments
- Systems administrators must receive standardized training and certification in the performance of IA functions and understand

the need for preparing readiness reports on the systems they administer

- The user community must be educated and certified to ensure necessary levels of competency
- Commanders and staff at all levels must understand the nature of the cyber domain of warfare and must be empowered to “Fight the Net” through shared situational awareness

The GIG is the net-centric warfare Center of Gravity... it must be protected.

IA is similar to operational security—everyone has a role, and each person must come to the realization that his or her participation is vital.



Just as you take personal responsibility for your weapon, you need to take personal responsibility for the security of the GIG.

The Mission Is Possible Because We Have a Plan

The GIG is the future of secured information for our armed services. When fully deployed and mature, it will serve as the net-centric source of trusted on-demand data and intelligence required by our joint, allied, and coalition forces to achieve

full spectrum dominance. A strong IA plan that includes personal vigilance on the part of all users is needed to provide security to the edge for the GIG and ensure that sensitive information is not compromised.

A Call to Action

A secured GIG cannot be achieved without the dedication and commitment of everyone.

It starts with you.

To effectively “Fight the Net,” warfighters and commanders must establish the climate, commit the resources, organize and train personnel, and take individual responsibility for protecting the GIG.

Protection of the GIG requires a strong IA plan that includes the following elements:

DoD IA Strategy and Vision

Long-term view (vision, goals, objectives, measures, metrics, and policy). *Responsibility of the Department of Defense OSD(III)/IA Directorate.*

Implementation Guidance

Integration and implementation oversight of planning, programming, budgeting, and acquisition strategy for IA. *Responsibility of the Defense-wide Information Assurance Program (DIAP) office.*

IA Component of the GIG Architecture

Building IA into the GIG (standards, requirements, technologies, and portfolio management).

Responsibility of the National Security Agency (NSA).

Defense-in-Depth

Operational guidance (education, training, and awareness).

Responsibility of the Joint Staff, U.S. Strategic Command and the Defense Information Systems Agency (DISA).

Daily Execution and Implementation

Involves a strong IA plan supplemented by personal vigilance on the part of all GIG users.

Responsibility of us all.

We can and must ensure Security to the Edge.



Personal involvement on the part of each of us is the only way to safeguard the GIG and the information that moves within it.



To learn more about Information Assurance and how it can support your specific mission, please contact:



IA Directorate of ASD(NII)
Directorate of Information Assurance
OASD(NII)/IA-Rm 3D239
6000 Defense Pentagon
Washington, DC 20301-6000
<http://www.dod.mil/nii>



The Joint Staff, J6 I&A
Integration and Information Assurance Division
Rm 1E588
6000 Defense Pentagon
Washington, DC 20318-6000
<http://www.dtic.mil/jcs/>
SIPR: <http://j6.js.smil.mil/>