OFFICE OF THE SECRETARY OF DEFENSE
1000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-1000

SEP 3 0 2015

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
CHIEF OF THE NATIONAL GUARD BUREAU
COMMANDERS OF THE COMBATANT COMMANDS
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER
ASSISTANT SECRETARY OF DEFENSE FOR LEGISLATIVE AFFAIRS
ASSISTANT TO THE SECRETARY OF DEFENSE FOR PUBLIC AFFAIRS
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Department of Defense Cybersecurity Culture and Compliance Initiative

The attached Department of Defense (DoD) Cybersecurity Culture and Compliance Initiative (DC3I) signed by the Secretary of Defense and Chairman of the Joint Chiefs of Staff directs U.S. Strategic Command (USSTRATCOM)/U.S. Cyber Command (USCYBERCOM) to lead DoD assessment and Service-coordinated implementation of DC3I principles and individual cybersecurity responsibility tasks in the next 180 days. As essential partners, however, the Secretary and the Chairman consider commanders and leaders from across the Department critical to DC3I success.

Please ensure widest dissemination.

Michael L. Bruhn
Executive Secretary

Attachment:
As stated

SEP 28 2015

The April 2015 Department of Defense (DoD) Cyber Strategy highlighted how the U.S. governmental reliance on the Internet and data systems leaves us increasingly vulnerable to cyber threats. The strategy guides cyber forces, strengthens our cyber defenses, and reinforces our deterrence posture. It sets clear, specific goals and supporting lines of effort for the Department to achieve over the next 5 years and beyond.

Technical upgrades and cyber organizational changes, however, are only part of the solution to reliable enterprise cybersecurity. Each of us, as network users and providers, has an individual responsibility to protect the Department of Defense Information Networks (DoDIN). Nearly all past successful network penetrations can be traced to one or more human errors that allowed the adversary to gain access to and, in some cases, exploit mission-critical information. Raising the level of individual human performance in cybersecurity provides tremendous leverage in defending the DoDIN.

This document outlines how we will transform DoD cybersecurity culture by improving individual human performance and accountability in mutual support of the DoD Cyber Strategy. We are calling this effort the **DoD Cybersecurity Culture and Compliance Initiative (DC3I).** The DC3I will permeate every corner of the "DoD Cyber Enterprise," which is defined as the totality of organizations and people—**leaders, service providers, cyber warriors, and general users**—who provide or use cyber capability to accomplish a mission. The DC3I is not intended to supersede existing efforts being undertaken by the Services and other elements of the DoD Cyber Enterprise. Rather, it is intended to enable and augment and, in some cases, reshape them at the individual human performance level.

DC3I establishes five operational excellence principles—**Integrity, Level of Knowledge, Procedural Compliance, Formality and Backup, and a Questioning Attitude**—that will be fundamental to the DoD Cyber Enterprise. These principles borrow substantially from proven initiatives in other high-risk endeavors that have inculcated high levels of personnel reliability into daily operations. The DC3I will further take a systems approach to education and training; scheduled and spot inspections; periodic and episodic reporting; and targeted investments that embrace mission-driven cybersecurity. The initiative makes clear that the Department is willing to accept some inconvenience to enhance our security posture.

U.S. Strategic Command (USSTRATCOM)/U.S. Cyber Command (USCYBERCOM) will lead the DC3I implementation. As essential partners, however, commanders and leaders from across the Department are the critical element to DC3I success. USSTRATCOM/USCYBERCOM, in coordination with the DoD CIO, will provide quarterly updates to the DepSecDef and VCJCS.

General Martin E. Dempsey
General, U.S. Army
Chairman of the Joint Chiefs of Staff

Ash Carter
Secretary of Defense

18

Department of Defense Cybersecurity Culture and Compliance Initiative (DC3I)

September 2015

The DoD Cybersecurity Culture and Compliance Initiative

Introduction

Over the past decade, Department of Defense (DoD) core functions have become increasingly reliant on the Internet and other networks at various classification levels. In addition to being central to the everyday operations of the Department, they enable a host of important information services across a vast number of different devices in support of management, logistics, budgeting, policymaking, personnel services, and other essential tasks.

The vulnerability of these networks has grown substantially in parallel with our increasing dependency on them. In some instances, threat actors have successfully penetrated our networks through multiple vectors to steal important information, expose non-public information, interfere with operations, and conduct other malicious activity. Potential adversaries likely view DoD's reliance on cyber—and its large threat surface area—as a strategic vulnerability they can exploit. We should expect a higher volume of concentrated network intrusions across all phases of conflict.

Across the DoD Cyber Enterprise, the battle for cybersecurity is constantly shifting as adversaries and defenders correspondingly innovate and adapt capabilities. The Department has invested heavily in cybersecurity solutions to protect our networks, including increased capacity for critical IT organizations, such as NSA and DISA, as well as technical investments like the Joint Regional Security Stacks (JRSS) that underpins the DoD's Joint Information Environment (JIE) security architecture. We have also invested in USSTRATCOM/USCYBERCOM and their Service Cyber Components, maturing capability and capacity to conduct global military operations in and through the cyberspace domain, in support of Combatant Command (CCMD) missions.

Expenditures in the cyberspace domain are beginning to provide measurable return on investment. Less than 0.1 percent of the 30 million known malicious intrusions on DoD networks between September 2014 and June 2015 compromised a cyber system. Indeed, we are interdicting more threats than ever before and threats that do penetrate our networks are quickly being contained. The defense of our DoDIN has never been stronger and our competency in defending critical infrastructure improves daily.

Despite these improvements, successful exploitation and unauthorized intrusions still occur on DoD networks—and roughly 80 percent of incidents in the cyber domain can be traced to three factors: poor user practices, poor network and data management practices, and poor implementation of network architecture. Thus, technical upgrades and cyber organizational changes are only part of the equation when it comes to protecting the DoDIN. A separate and significant challenge is identifying and protecting against harm due to human error by both IT professionals and the great number of everyday DoD users.

In contrast to the other warfighting domains (e.g., maritime, land, air, and space), intrusions in cyberspace may not always result in visible, physical damage. It can be easy for users to underestimate the harmful effects of an intrusion enabled by human error—whether caused by

inaction or inappropriate action. In cyberspace, the tangible mission risks of poor individual cyber behaviors are difficult to see, feel, and interpret. Even more, the loss of information or exploitation of technical vulnerabilities made possible by an unauthorized intrusion on the DoDIN can lie dormant for days, months, or years before an adversary makes use of them. Thus, in the tradeoff between operator convenience and security, the former tends to dominate to the detriment of the latter.

There is also often a lack of recognition and, in some cases, denial that human error may have been the root cause for a successful network intrusion in the first place. The failure to recognize this cause and effect relationship leads individuals to sometimes place personal convenience ahead of operational security or to regard information systems with less care and caution than they would a kinetic weapons system. On a daily basis, our workforce and Warfighters unintentionally put mission-critical information systems at risk by treating them as though they are not vulnerable to adversary exploitation.

In other DoD domains, reporting and accountability, constant assessment, and learning are driven by engaged leaders who instill and reinforce the behaviors necessary for our wartime readiness culture to thrive at the individual level. We do not yet have that same culture for cybersecurity. DoD cyber capabilities, ubiquitous cyber-infused mission systems, and cyber-enabled business and enterprise-wide network operations were delivered to DoD gradually and built up over time. Consequently, a definitive cybersecurity culture that addresses human performance and the vital role of the individual in our cyber-readiness fabric was never instituted on par with the collective importance that information systems have assumed.

The imperative is clear: DoD needs to fundamentally shift cybersecurity cultural norms from the most senior leaders down to the unit and individual level. Like a military weapons system, DC3I calls for the DoD Cyber Enterprise to treat access to DoD networks with the highest standards of individual knowledge, accountability and reliability. Network access must be dependent on deliberate, disciplined and effects-focused cyber behavior.

All of us within the DoD Cyber Enterprise must understand the operational excellence principles and individual cyber norms of behavior necessary to protect our DoDIN and mission critical cyber infrastructure.

Operational Excellence Principles

The behavior of the DoD Cyber Enterprise will be based on five time-tested operational excellence principles, drawn from other enterprises that successfully manage critical technical systems, such as the U.S. Nuclear Navy. These principles are intertwined and highly dependent upon each other. They will be part of cybersecurity training, and will be understood—and adopted—by those who are authorized to use the DoD's information technology and mission systems. When consequential human error is discovered, it should be debriefed and reported in keeping with these principles. The principles are described as follows:

- Integrity is the first and most fundamental principle of our cyber operations. It is demonstrated by individuals who are diligent in following best practices for cybersecurity

and who readily bring their mistakes to the attention of their supervisors, and units that report their incidents to the chain of command. When integrity is strong in an organization, people deliberately refuse to compromise security for convenience, and much less time is spent on analysis to find the source of a problem. The workforce is accordingly characterized by a resistance to knowingly doing the wrong thing, such as downloading software, accessing inappropriate Web sites, and using portable memory devices. This honesty in reporting benefits the entire enterprise, empowering people to report their mistakes. A healthy culture is one in which self-reported errors are the norm for individual and organizational learning; gross negligence and malfeasance or attempts to withhold known mistakes are met with appropriate action.

- Level of Knowledge enables all of the other principles. It starts with ensuring our operators and Warfighters have the information needed to function safely on our networks and systems. Such knowledge will guide daily behavior on the network and minimize threat surface and risk. It empowers us to recognize when something is wrong and to make appropriate decisions if an incident is not covered by a specified procedure. This cyber competency will be cultivated through both baseline education and frequent refresher training. It will be a living and learning process that adapts as both the cyber domain and threat landscape changes. Knowledge of cyberspace, by both network users and providers, instills confidence and an ability to identify and appropriately address threats, which will make us more effective at advancing cybersecurity competency across the Department. Thus, IT professionals must be appropriately identified in manpower databases, have exceptional initial and continuing education and training, and be appropriately certified. All of us within the DoD Cyber Enterprise must also have a fundamental understanding of: how networks and mission-systems connect and are protected, what makes our networks vulnerable and how adversaries penetrate them, the types and consequences of an unauthorized DoDIN intrusion, and the kinds of network behavior that should draw suspicion among users. The greater our collective competency in cyberspace, the better prepared we are to mitigate risk, make smart decisions, and achieve mission objectives during an unauthorized DoDIN intrusion.

- Procedural Compliance means practicing the proper procedures vice taking shortcuts on cyber systems that are vulnerable to exploitation. It is thinking before we act (for example, before clicking on a suspicious e-mail) and conforming to known cybersecurity requirements (such as using a PKI certificate for two-factor authentication). For our IT professionals, it means ensuring all cybersecurity compliance directives are completed and up-to-date on all systems. It also means bringing to light and properly modifying procedures that are ineffective. Most importantly, it means elevating noncompliance and resource deficiencies to senior leadership. Failure to maintain the discipline of compliance, in other, more physical disciplines is written in blood; in cyberspace, it is written in compromised information and missions. Compromise in either can cause mission failure and loss of life.

- Formality and Backup improves the resiliency of our mission critical cyber infrastructure and protects against a lax atmosphere that leads to complacency and misunderstandings. It calls for using two-person integrity whenever a procedure is conducted that exposes the

network to higher risk; backing each other up and providing technology-enabled oversight of network behavior; proactively discussing and adjusting potential process problems early; and providing timely assistance to users when they have a problem or detect suspicious activity. For example, when a network sensor detects that an unauthorized device is connected to the network, both IT professionals AND leaders must immediately and aggressively investigate where and why the incident occurred. We must maintain an appropriate level of vigilance across the DoDIN at all times.

- A Questioning Attitude is empowered by knowledge. It means following warning signals to the source and using experience and level of knowledge to take action when there are indicators that something does not seem right. Its friend is mental discipline; its enemy is mental laziness. It means *interpreting* what we see—such as a suspicious e-mail or unusual network behavior—rather than just *accepting* it. It is checking our work, remaining alert, and never being satisfied with an answer that is anything less than rigorously analyzed.

The DoD Cyber Enterprise

In building a strong cybersecurity culture, we will specifically account for each of the different populations that use DoD networks and mission systems, including their particular needs, vulnerabilities, risk profiles, and expectations associated with cybersecurity discipline. USSTRATCOM/USCYBERCOM have identified four distinct groups within the DoD Cyber Enterprise: leaders, providers, cyber warriors, and users. Increasing individual competency, while also reducing human error within all of these populations, is essential to mitigating cybersecurity and mission assurance risk across the Department. Our understanding of each of these groups—and the different strategies required to improve individual performance—will grow over time.

- *Leaders*: Commanders and those who hold positions of responsibility and authority across the Department are charged with ensuring the DC3I becomes a prominent element of our approach to cybersecurity. They will lead our change efforts and ensure adequate resourcing of capabilities and capacity that improve cybersecurity. Leaders will be held accountable by the chain of command for the cybersecurity performance of their organization and the individuals who comprise it, and for the role cybersecurity performance plays in accomplishing assigned missions. Leaders will set an example and help individuals master appropriate cyber behavior. They will take action against those who commit gross negligence or errors of commission; they may use all available means, both legal and administrative, as they deem appropriate.

- *Providers*: At the core of systems and networks are government workers and contractors who design, build, secure, maintain, provision, and operate them—the "Providers"—which includes system engineers, administrators, materiel providers and IT professionals. They are a group of highly trained and educated IT professionals expected to perform at the highest levels. Deliberately and systematically reducing human error in this "inner circle" is absolutely crucial, as their professional competency has enormous consequences for our mission success. When our systems and networks are properly configured, patched and resilient, we deny our adversaries the benefit of easy access and we retain freedom of

maneuver in cyberspace. However, when our systems and networks are exposed, vulnerable, misconfigured and not optimized for defense, the risk to the mission and our forces is grave and our adversaries gain the initiative, impose high costs or risks, and deny us our freedom of maneuver. The providers must embody and exude our cyber operational excellence principles, continually improve their knowledge and understanding of our systems and networks, and employ their skills in innovative ways to proactively mitigate risk and deliver mission assurance through secure and resilient networks across the Department. These professionals literally have the keys to the cyber kingdom and must be held personally accountable for failures to adhere to the highest standards of cybersecurity best practices.

- *Cyber Warriors*: Cyber Warriors include the Cyber Mission Force Teams, DoD Cyber Red Teams, and other cyberspace defenders such as Computer Network Defense Service Providers (CNDSPs), which conduct cyberspace operations in and through the domain. These cyber warriors must be trained and educated to deliver effects through cyberspace to achieve assigned mission objectives. They are our "trigger pullers" in cyberspace and they maneuver within the domain to deliver effects and to counter adversaries. They have enormous responsibility for the proper, safe, and lawful employment of their capabilities. Their daily "hands-on" interaction with our cyber weapon systems aligns them closest to the classic warfighting communities within DoD. Warfighting mission readiness is one of their key measures of effectiveness. As such, cyber warriors must embrace a culture of training, education, exercises, continuous learning to evolve effective tactics, techniques and procedures, sound operational risk management, and routine evaluations of compliance and operational effectiveness. These teams must thrive on professional competency, discipline, innovation and teamwork, as well as a comprehensive knowledge of the application of Joint combat power.

- *Users*: These are the vast number of Service members and civilians who rely daily on cyberspace for mission assurance and mission success, but who as individuals have no dedicated, assigned mission in the domain. Nevertheless, user behaviors play a key part in keeping intruders out and stopping them quickly should they get in. While it is unrealistic to expect this broad set of users to possess the same expert knowledge as IT professionals, they must be expected to maintain sufficient cyberspace knowledge and understanding to operate and protect the DoDIN with good cyber hygiene at the individual user level. It is essential that all DoD Cyber Enterprise users know their ownership role in protecting the networks, systems, and devices they use. When asked, each of us should be fluent on the importance of security, the fundamentals of how security can be compromised, and the protocols for cyber hygiene behavior on the network. Users must be held accountable for actions on the network, including negligence and violations of established protocols. It is important to communicate frequently with users and to provide the requisite training to maintain their awareness of their important role. Similar to other areas such as rifle marksmanship, we will establish incentive systems for users who demonstrate knowledge and performance beyond the minimum expectation.

Implementing and Resourcing the DC3I

Improving our culture of cybersecurity requires a holistic approach that addresses people, processes, and technology—there is no silver bullet in any one area.

Implementing the DC3I will not be easy; it requires significant effort along three main non-materiel lines of effort and two materiel lines of effort, as well as sufficient resources to achieve success. Realizing the objectives of DC3I will require sufficient investment to improve our culture across the breadth of the DoD in which every individual is a part of the DoD Cyber Enterprise.

Non-Materiel Elements

The primary non-materiel elements that must be quickly implemented fall along the three main lines of effort of Cyber Training, Education, and Leader Development; Cyber Inspections; and Cyber Reporting and Accountability.

Cyber Training, Education, and Leader Development

Good training is foundational to the necessary cultural shift needed for cybersecurity awareness and effectiveness. Because the principle of "level of knowledge" is so interconnected with the other principles, quality cyber training and education is essential for cyber Leaders, Providers, Warriors, and Users alike. Each of these groups has significant responsibilities for what they do or do not do on the systems and networks. An improper action by any one individual from within these groups can affect the entire DoD Cyber Enterprise. Therefore, DC3I will be built upon a foundation of both individual and collective training.

- Individual Training

  - *Leaders*. Commanders at all levels need additional training to understand, assess and interpret cyber reportable events and incidents and how they impact operations. Commander's Critical Information Requirements (CCIRs) should include Cyber Warrior-informed reporting criteria, allowing more complete understanding of mission risk. Commanders have the responsibility to emphasize cybersecurity awareness, to include individual user accountability, training, and leader development.

  - *Providers*

    - System engineers in our acquisition and research and development communities require the knowledge necessary to build defensible systems from the start. This group must understand that basic investments in secure design today will significantly reduce the cost of protection once the system is deployed. We can no longer afford to overlook cybersecurity requirements to support convenience in maintenance or to expedite deployment of new capabilities.

- Training for administrators and IT professionals must be timely, adequate and recurring. It is imperative that training is aligned to a hierarchy of industry standards, like Security+ and Certified Information Systems Security Professional (CISSP). Streamlining the processes for getting appropriate certifications and credentials across the force will achieve maximum proficiency. The cultural focus of this group's training will be on ensuring system administrators know they are our most critical line of protection. The group needs senior leader support for a shift in emphasis from convenience to security, while balancing mission risk and mission assurance. For example, if a Web portal is offline for patch maintenance, there will not be pressure to place it back online prematurely or to ignore needed updates. Both system administrators and materiel providers must be given the resources they need to effectively perform their mission and must speak up if budgetary or other organizational pressures are impacting cybersecurity.

- *Warriors*. This warfighting group and the providers are mutually supporting and must learn from each other. Sophisticated sensors and warning systems allow Cyber Warriors to see threat vectors early. Sharing that information rapidly with providers will enable us to better manage network defense infrastructure. Cyber Warriors have a long training pipeline, with Service schools providing an initial baseline of IT proficiency and numerous joint schools teaching highly specialized tactics, techniques and procedures. The key cultural principle to instill throughout this training is integrity. While all of these personnel are highly skilled, they must be prepared to transfer to other cyber teams throughout their careers and support cyber operations around the world. This requires a uniform, integrated approach to training throughout the Cyber Enterprise.

- *Users*. This is the largest, most diverse group for cybersecurity training. Since level of knowledge is an important interlocking cultural principle, high-quality cybersecurity education is critical to this group's success. Moving beyond "Web-based training with a six question quiz" will send a message that cybersecurity training is an important priority for the entire DoD Cyber Enterprise. Web-based education must become more frequently recurring and relevant to changing threats; it must be embedded with day-to-day operations on the network. The training must advance user knowledge, maintain baseline competencies, and incentivize higher levels of comprehension. Additionally, a cultural shift requires personal leader engagement and supervision at all levels. It necessitates discussion and action among peers. All training should be reinforced by face-to-face discussions and interactions based on recent and relevant events. Continuing cyber education should ensure that each user understands his or her full accountability for actions or inactions on the network.

Task 1. Within 120 days, USSTRATCOM/USCYBERCOM will develop cybersecurity training briefs, with associated talking points, for Combatant Commanders, Services, Agencies, and all other DoD Components to use in leadership training.

Task 2. Within 120 days, USSTRATCOM/USCYBERCOM and DoD CIO will direct the appropriate stakeholders to develop educational and training requirements for cyber Providers.

Task 3. Within 120 days, DoD CIO will implement engaging scenario-based training to educate users on potential mission impacts as a result of failures to follow cybersecurity procedures.

Task 4. Within 120 days of receiving the deliverables from each Task (1-3), Combatant Commanders, Service Chiefs, Agency, and DoD Component Heads will take appropriate actions to incorporate the DC3I principles into all levels of training, including, but not limited to accession pipelines, professional development, and leadership development.

- Collective Training. Altogether, our networks comprise a warfighting enabling capability and a key force multiplier. When we employ cyber capabilities securely, we are more fully able to leverage our networked warfare advantage. The reverse is also true. Collective, mission-driven cyber training involves both competent cyber mission forces or teams and emphasizing cyber cultural norms of behavior. Realistic cyber events must be infused into all aspects of operational training, from USSTRATCOM/USCYBERCOM and CCMD exercises to Service-level tactical events. Operational and tactical commanders and leaders need to interpret and assess the kinetic effect that cyber insecurity may have on the mission; they also must take the opportunity to integrate cyber effects into mission planning. Until training and exercises thoroughly demonstrate the debilitating impacts of adversary cyberspace operations on a unit's ability to project power forward, commanders and leaders cannot understand the potential for failure. Kinetic and non-kinetic cyber capabilities must become routine, like normal fire support coordination at the tactical level and targeting boards at the joint task force level. Cybersecurity must become as integral to operations as a tactical unit's scheme of maneuver. Only in this manner will the culture of cybersecurity and employment be inculcated into the DoD and its warfighters.

Task 5. Within 120 days, CJCS will develop and implement criteria for assessing Combatant Commander and Service efforts to integrate cybersecurity into operational training and exercises.

Cyber Inspections

Ensuring the Joint Force and its supporting entities are performing to standard is a vital part of driving human error out of our operations and will ultimately improve our cyber culture. Although the term "inspection" often suggests overbearing supervision and bureaucracy, it is necessary to determine whether the Enterprise is effective. Inspecting cyber performance on a regular basis will keep IT professionals, users, and leaders engaged in ensuring that we are meeting the standards associated with good network order and discipline. Inspections also reveal best and worst practices or emerging challenges that can be implemented across the DoD Cyber Enterprise, as well as systemic issues that require resolution.

Two types of mutually supporting inspections will be conducted by and within the DoD Cyber Enterprise: 1) scheduled inspections conducted by DISA with oversight from JFHQ DoDIN and 2) no-notice spot checks performed by DISA or the Service Cyber Components. During inspections, corrections should be made on the spot (when feasible). When the situation dictates, outside resources may be required to mitigate unacceptable risk to the network.

Leveraging technology can help in three ways: 1) automating inspections to reduce required manpower and increase the number of inspections; 2) ensuring real-time, continuous network monitoring; and 3) establishing a collaborative Cyber Threat and Incident Common Operational Picture where IT Providers and Cyber Warriors can post trending problems, signatures and solutions. The JS J-6 will reinforce identifying and sharing trends through inclusion in its quarterly assessment disseminated to the Joint Force.

- Scheduled Inspections. Each military or civilian entity (to include cleared defense contractors using the DoD systems) deemed by USSTRATCOM/USCYBERCOM and JFHQ DoDIN to be conducting cyberspace operations at a level that requires inspection will submit to a scheduled inspection event at least once every 2 years. Inspectors should be individuals who have deep experience in cybersecurity and should be considered elite members of the DoD Cyber Enterprise. Units will have the opportunity to prepare for these inspections and will have full knowledge of the checklist used by the inspection team. Although organizations should maintain a philosophy of being "always ready" for an inspection instead of "sprinting down to the wire," scheduled events will include an incentive system for those that demonstrate distinguishably high standards.

- No-Notice Spot Checks. No-notice inspections will be randomly performed by qualified inspectors who have been trained to the same standards as scheduled Cyber Command Readiness Inspectors. Spot check inspectors will be granted access at any time for such an event. The inspections should focus principally on compliance with cybersecurity directives, network configuration, other system administration responsibilities, and general cyber hygiene. The lead IT professional in a unit that has been spot checked will be required to make contact the following day with the lead of the inspection team to address correction of any deficiencies found during the check. Spot checks have the benefit of reinforcing standards during interim periods between scheduled inspections. Further, they efficiently employ our finite inspection teams by conducting shorter, less comprehensive inspections that quickly review and correct high-priority vulnerabilities. Spot checks can be random or generated by events and activities that leadership believes require extra attention.

Task 6. Within 180 days, USSTRATCOM/USCYBERCOM and JFHQ DoDIN develop a resourcing plan to support scheduled inspections and no-notice spot checks as outlined above. The resourcing plan will include the methodology used to determine which entities require scheduled inspections every 2 years and any investments in technology that can help automate the cyber readiness inspection/assessment process.

Cyber Reporting and Accountability

It is necessary to understand how the elements of the DoD Cyber Enterprise are performing and what types of issues individual entities are experiencing. As such, a formalized reporting system within the Enterprise will consist of periodic and incident reports as follows:

- Periodic Reporting. Each entity that is subject to a scheduled cybersecurity inspection will provide a quarterly report to USSTRATCOM/USCYBERCOM signed by the commanding officer or senior civilian, and capturing the unit's performance over the previous quarter. These reports will include a summary of training conducted, relevant statistics that will better enable USSTRATCOM/USCYBERCOM and JFHQ DoDIN to track individual operator and network performance, and any issues for which the unit needs assistance.

- Incident Reporting. We will implement a system of incident reporting that involves a complete description of the incident, a thorough exploration of its causal factors, a reasoned approach for mitigating and preventing recurrence, a summary of accountability actions taken (where appropriate), and/or recommendations on procedural lessons learned for enterprise-wide dissemination. All incidents should be diagnosed in terms of the **operational excellence principles** as part of the causal factors analysis. The DoD Cyber Enterprise will be dependent on adherence to the operational excellence principle of "integrity" as a non-negotiable imperative for commands to accurately report incidents. Units identified as having failed to do so will be held accountable. USSTRATCOM/USCYBERCOM will provide guidance regarding both the process for reporting and specific criteria that constitutes a reportable incident. For example, isolated negligence with no significant consequence is likely too low of a threshold for reporting, while limiting incident reporting to major network intrusions is too narrow. Commanders' judgment will be critical in applying USSTRATCOM/USCYBERCOM guidance. USSTRATCOM/USCYBERCOM will also provide guidance on the structure and content of incident reports.

Task 7. Within 90 days, USSTRATCOM/USCYBERCOM promulgate the format and process for submitting quarterly reports from inspected units.

Task 8. Within 60 days, USSTRATCOM/USCYBERCOM provide updated format and process for Incident Reporting.

Materiel Elements

The DC3I borrows substantially from other initiatives, like the nuclear propulsion program, that have inculcated high personnel and organizational reliability into daily operations. Like these other initiatives, the DC3I will require some materiel investment to enable the human element to succeed. In order to maximize the effect of this initiative, materiel elements must be leveraged to make human error less likely and less dangerous.

There has been no "free lunch" in past initiatives and there will be no free lunch in the DC3I. One rule of thumb in the IT arena is that every $1 spent to prevent cybersecurity intrusions saves

$7 in clean up. The growing number of cyber intrusions across the Department is costing tens of millions of dollars and thousands of man hours to remediate. It is a worthwhile investment to fund the required materiel elements of the DC3I, as well as enterprise technological solutions that are on the horizon—like the JIE.

Two of the primary DC3I materiel elements that must be implemented are focused on the "Provider" group and fall into the areas of 1) adequate capabilities, authorities and architectures, and 2) sufficient human resources for providers to execute the numerous and rapidly increasing number of security mitigations, patches, updates, and upgrades continually required across the DoDIN, to include mission systems, within mission relevant timelines. The last materiel element is associated with the resources needed to create and manage the overall initiative.

Adequate Capabilities, Authorities and Architectures

The many benefits of cyber culture change in the human dimension are bounded by significant and growing cyber materiel gaps. There are inadequate capabilities, authorities and architectures to reliably monitor and remedy enterprise configuration and patch requirements. USSTRATCOM/USCYBERCOM and DISA jointly manage the Information Assurance Vulnerability Management (IAVM) program that identifies and publishes vulnerabilities or relevant directives. Due to the complexity of our hardware and software systems, and the large number of vulnerabilities that are continually discovered, there is a constant and increasingly critical demand on providers to implement multiple IAVM tasks across large and diverse networks. Many providers have to manually scan and patch every single device for all newly received IAVM. This touch labor is expensive, time consuming and leaves a backlog of unmitigated vulnerabilities.

Additionally, segmented networks and domains often contain enclaves that are partitioned away from the main network and operate under different authorities that prevent providers from making updates. For example, a weapons system program management office that is concerned a new patch will negatively impact a legacy system's functionality may decide to forego a needed update without fully understanding risk implications as a whole. In some cases, there is insufficient sustainment funding for these programs to appropriately test and apply such needed patches; this has the potential to unintentionally put the security of the entire DoD Cyber Enterprise at risk.

Task 9. Within 180 days, USSTRATCOM/USCYBERCOM and DoD CIO will lead an assessment and provide recommendations for the changes that need to be made to capabilities, authorities and network architectures that would enable providers to execute their tasks within mission relevant timelines.

Sufficient Human Resources for Providers

As a result of recent fiscal uncertainty, there are significant risks that exist today which will not be completely mitigated until the JIE is fully implemented. For instance, our currently fragmented networks require intensive manpower support, yet providers have been forced to reduce costs and manning for a number of years. In many cases, significant cuts have been made

to the provider workforce and their units. Often times, an entire installation will only have a limited number of personnel to execute critical provider tasks associated with ensuring systems and networks are properly configured, patched, diversified and resilient. When combined with the previously highlighted constraints to ensuring adequate capabilities, authorities and network architectures, the lack of sufficient personnel makes it difficult to keep up with requirements to maintain good cybersecurity.

Task 10. Within 90 days, USSTRATCOM/USCYBERCOM and DoD CIO will lead the initial assessment and provide recommendations for what impact human resource shortfalls, to include recruitment and retention, have on the ability of providers to execute their tasks within mission relevant timelines and to recommend corrective actions to remedy these shortfalls.

USSTRATCOM/USCYBERCOM, as DoD's cyber domain mission leaders, will lead the DC3I implementation. The management of all DC3I elements will include the need to create, manage, oversee, and assess improved Cyber Leader Development, Training, and Education programs; a much more robust and intensive Cyber Inspections regime; and a more complete Cyber Reporting and Accountability program, as well as working the detailed technical issues associated with overcoming materiel deficiencies that prevent the successful implementation of a robust cyber culture.

Task 11. Within 90 days, USSTRATCOM/USCYBERCOM provide an assessment and recommendations for what resources (dollars and people) are required to stand up the capability as the DC3I mission owner. This assessment must be in coordination with the CJCS Joint Staff.