REPORT TO CONGRESS

A REPORT IN RESPONSE TO REQUEST ON PAGE 323 OF
SENATE ARMED SERVICES COMMITTEE REPORT NUMBER 110-77

DEPARTMENT OF DEFENSE
PERSONNEL ACCESS TO THE INTERNET

September 2007

Report to Congress on DoD Personnel Access to the Internet

Table of Contents

Report to Congress on Personnel Access to the Internet

1. Purpose (U)

(U) This document is in response to the request on page 323 of the Senate Armed Services Committee (SASC) Report 110-77, which states:

> *(U) The committee is concerned with the recent Department of Defense policy changes that seek to limit the access of military personnel to certain popular internet web sites. While the committee understands the need to preserve available bandwidth for military needs and the necessity of ensuring operational security, the potential negative effects on morale must also be carefully considered. Those deployed in Iraq, Afghanistan, and elsewhere around the world, sometimes for more than a year, deserve every opportunity to connect with their friends and family on a frequent basis. Social networking web sites facilitate that communication for this generation, in the same way letters, phone calls, and telegrams did for previous ones. The committee believes that access to the commercial internet can promote strong morale among personnel in the field as well as family members on the home front.*
>
> *(U) The committee directs the Secretary of Defense to develop a report that includes a detailed description of the measurable effect that the use of these sites has had on operations and a detailed analysis of any bandwidth or security challenges that their use poses, as well as a description of any policies and procedures in place for the provision of internet access for deployed personnel when operational security requires denial of access via Government systems. The report should be delivered to the congressional defense committees no later than September 1, 2007.*

(U) This report examines the effects that the use of social networking sites has had on operations, an analysis of the bandwidth and security challenges that their use poses, and a description of the policies and procedures in place for the provision of internet access for deployed personnel when access to Government systems is denied. Access to a targeted list of social networking web sites has been blocked to free mission-related bandwidth and ensure the availability and integrity of Department of Defense (DoD) networks. Supporting material accompanies this report including a classified appendix. A description of the policies on the protection of sensitive information is also included.

(U) In summary, DoD must take actions to configure its networks to optimize the flow of operational information and reduce exposure to an ever-increasing body of threats that may be introduced via social networking sites.

2. Background (U)

(U) In today's global environment, it is vital that DoD maximize the availability of network resources and efficiencies across its Global Information Grid (GIG) in support of efforts to defeat terrorists and their organizations. The DoD will continue to take all actions necessary

to assure the operational availability, delivery, and protection of its information resources, working toward strategic improvements while confronting evolving threats.

(U) The Department's decision to "block" access to certain social networking sites is actually a filtering action designed to limit wholesale access to recreational web sites. The risk of social networking sites is commonly known and commentators caution enterprise managers on the disproportionate consumption of network resources by recreational web use and the potential for social networking sites to serve as a conduit for malicious code. Internet Protocol (IP) filtering is the most cost-efficient and time-responsive tool to help ensure the GIG is available and secure to support current and future warfighter and mission support requirements.

(U)This action was undertaken only after extensive internal coordination and careful consideration of its potential consequences, especially as they relate to deployed personnel. Web filtering is not meant as an indictment of a particular group of sites, but rather it is part of an effort to proactively defend the DoD's information technology resources and to ensure sufficient bandwidth capacity for developing Defense programs. As user demand for network resources continues, the DoD will continue to use management controls such as web filtering, but will also make prudent investments in infrastructure to ensure ongoing network availability for DoD missions. The effect of such actions on morale and welfare of deployed military personnel will continue to be key consideration before taking any such actions.

3. DoD's Rationale to Filter Web Sites (U)

3.1 Web Filtering Consistent with DoD Network Policy(U)

(U) DoD policy provides for a "defense-in-depth" strategy, using risk-management principles to defend against both external and internal threats by employing multiple protections at different layers within information systems and computer networks (DOD Instruction O-8530.1, "Computer Network Defense").

(U) By the policies listed in Appendix A, the DoD exercises vigilance over its networks, assesses vulnerabilities as they evolve, and makes corrective inputs to preserve and optimize the flow of mission-related, operational content.

(U) These policies allow organizations to configure their networks as operational conditions dictate. For example, streaming audio and video sites—including *youtube.com* and *myspace.com*—were restricted by local policy in the Central Command (CENTCOM) area of responsibility in Iraq and Afghanistan for years prior to the broader DoD filtering action.

3.2 DoD Web Filtering Supported by Industry Trends and Evolving Threats (U)

(U) Current industry and academic literature cautions information technology professionals on the proliferation of both streaming media and social-networking sites—the bandwidth they consume and the potential vulnerabilities they bring to the enterprise. One such caution was issued in a November 2006 McAfee report entitled "Top 10 Security Threats in 2007." These types of cautions led the DoD to analyze the potential impact recreational web

traffic has on its aggregate network, both in bandwidth consumption and potential security vulnerabilities (Appendix B).

3.3 Recreational Internet Use and Bandwidth Consumption (U)

(U) Preserving bandwidth is a critical consideration for the DoD. The GIG includes over 12,000 local area networks connecting approximately 5 million individual computers. It is a distributed and heterogeneous—versus homogeneous—entity. At its backbone, the GIG's capacity is in the gigabit range, whereas at the tactical edge, in deployed locations, network availability can be reduced to megabits or kilobits. The personnel who serve at the tactical edge who experience significantly reduced bandwidth, potentially derive the most operational benefit from web-filtering actions.

(U) The GIG supports a variety of network-intensive applications ranging from combat operations and command and control to logistics and general support. The GIG itself is a stage for organizational transformation, and must accommodate a more "Department-wide enterprise net-centric approach" which will be heavily dependent upon available throughput (Quadrennial Defense Review 2006). The Army, Navy and Air Force are thus engineering their future architectures on the assumption that DoD infrastructure will support its growing operational net-centric requirements.

(U) The GIG possesses finite capacity, at times requiring difficult resource allocation decisions, and operational content continues to grow. Sensors such as unmanned aerial vehicles now offer unprecedented levels of still and motion imagery to a wide audience of mission stakeholders, but consume a great deal of the fixed bandwidth available. Additionally, the DoD is embarking on a near-term data sharing strategy that seeks to reduce Departmental costs by virtually bridging personnel worldwide and obviating the need for extensive travel and expense. This state-of-the-art collaboration environment requires a host of robust applications that will depend upon the ready availability of bandwidth.

(U) Thus far, limited collaboration pilots are promising. In October 2006, the DoD brought numerous geographically dispersed Stryker Brigade combat units together in a carefully managed collaborative session, the first of its kind. While the outcome of the event was generally positive, it required extraordinary efforts, which included adding bandwidth into some locations. It should be noted that as hundreds of other such events begin to take place across the network, the GIG must possess the ability to absorb this exponentially heightened volume of network activity.

(U) Based on the growth of these and other network-based services, DoD's demand for bandwidth essentially doubles every two years, far outpacing both current and projected GIG throughput. While programmed investments are being made to expand GIG capacity, they alone are not enough to appreciably slow the trend line that reveals an inevitable and imminent point at which the GIG will reach saturation (usage graph provided in separate classified appendix). Exacerbating this trend is the widespread use of the commercial Internet from GIG terminals. DoD network engineers have recorded instances where Internet traffic has saturated many of the GIG's 19 Internet Access Points (IAPs), often in association with non-DoD events that prompted a high volume of web interest. For example, following the Virginia Tech shootings in May

2007, several IAPs experienced saturation throughout the day because of heavy, sustained demand for commercial news feeds. Even more telling, the GIG experienced a 7 percent surge in Internet traffic corresponding to the tip-off of the 2006 NCAA Tournament.

(U) This looming network saturation, combined with the indicators of recreational Internet use, have compelled the DoD to exercise focused custodial responsibility over its information resources, addressing first the steady rise in commercial Internet access by GIG users. In order to preserve throughput and slow the growth curve in overall demand, the DoD began examining ways to temper the impact of inherently recreational Internet activity without impeding legitimate, mission-related web browsing.

(U) In the first of a series of deliberate steps to determine the gross amount of commercial Internet traffic entering the GIG's IAPs, analysts began to measure the degree to which web browsing is present on the network. The initial focus of the analysis was based not on site content, but simply on the raw, aggregate flow of Internet-to-GIG activity. A July 2006 engineering study revealed that approximately 90% of inbound Internet traffic is commercial web browsing, with a significant portion (as much as two-thirds) known to be for recreational use (see classified appendix). At its peak, this commercial web traffic consumed a sobering 2 gigabits per second, primarily during normal CONUS duty hours, bearing out many of the surges and saturation instances network analysts had previously recorded.

(U) Refining their focus even further, analysts translated their data into a list of commercial Internet domains, sorted in order of resources consumed. These sites served as grist for further analysis, and were ultimately distilled into a list of 13 candidates that could be readily identified as "recreational," and therefore unlikely to support any military application. Engineers concluded that the filtering of these sites would free bandwidth for operational use and surge capacity, while at the same time allowing GIG users continued access to all web sites with mission-related potential.

3.4 Security Threats and the Attack Vector of User-Contributed Media (U)

(U) While the ever-increasing demand for bandwidth drove much of the DoD's filtering rationale, computer security was yet another key concern. Because of the sensitive nature of Defense information and the fundamental need to maintain confidence in the network, DoD's network personnel ensure all potential vulnerabilities are fully explored and mitigated to the greatest extent possible. Known vulnerabilities are subject to exploitation by a wide and active array of hostile actors, from recreational hackers, self-styled cyber-vigilantes, various groups with nationalistic or ideological agendas, cyber criminals, transnational actors, and nation-states (see classified Appendix E).

(U) Commercial Internet security companies have consistently expressed concerns over the vulnerabilities associated with the types of recreational sites chosen for filtering by DoD, which are largely composed of user-defined content (e.g., social networking). Unclassified commercial threat reports estimate that up to one in every 600 social networking pages hosts malware. The increasing popularity of user-contributed web services is placing web filtering and antivirus solutions at a disadvantage in the battle to maintain the integrity of the Internet. Many

security solutions rely on URL databases that are relatively slow to react to the dynamic nature of the web content on these sites, thus rendering them ineffective.

(U) The challenge for the DoD comes from the unregulated nature of recreational sites. Unlike sites such as *microsoft.com,* where the content is controlled by the owner, thus providing a reasonable expectation of safe browsing, the content on many recreational sites is unregulated, user-contributed and constantly changing. The dynamic nature of these sites facilitates threat actors' ability to embed their malicious code within the content and affect a larger population. Recently, *myspace.com* was attacked by an Internet worm that was designed to steal login and password information from *myspace.com* users. The worm was so effective that when an informal scan of 150 profiles was conducted by a commercial security company, it found that almost one-third of the profiles were infected by the worm. This is especially disturbing since the program not only captured login credentials, but also sent e-mail embedded with malware from the compromised system to other people in the user's contact list, making it self propagating.

(U) Although DoD was not the target of this activity, the end result to the GIG would remain the same. A threat actor with the intent to gain unauthorized access to DoD systems could easily replicate this activity using socially engineered content. When the content is designed to entice DoD personnel, this type of threat becomes particularly problematic. In the end, the DoD's actions were prudent and not unlike those taken by many corporations who are already going to great lengths to reduce there exposure to the increasing variety and numbers of Internet threats.

4. Consideration of Operational Impact and Potential Effect on Deployed Personnel (U)

4.1 Operational Considerations (U)

(U) Motivated by engineering data on the volume of commercial traffic and the potential threats introduced by social networking, DoD information security personnel set out to determine the operational consequences that might result from targeted recreational web filtering. Rather than impose a wholesale blocking order, the DoD weighed operational considerations in order to accommodate exceptions and grant access to Defense entities with a compelling mission need for these sites. Given that some audiences within the DoD maintain a genuine need to access recreational sites for limited operational purposes (e.g., public affairs), a number of these organizations were exempt from the filtering action.

4.2 Potential Effects on the Morale and Welfare of Deployed Personnel (U)

(U) A primary concern prior to filtering was ensuring the continued ability of deployed personnel to maintain contact with family and enjoy recreational use of the Internet. Today, commercial Internet access is widely available to deployed personnel throughout Iraq and Afghanistan, as well as many other worldwide locations, many of which are paid for and established by the DoD itself. These Internet cafe sites do not rely on military networks for personal use, and thus fall outside the purview of DoD GIG policy. All IP service for these Internet cafes is provided by network connections outside the DoD-owned infrastructure.

(U) Internet cafes are extensively used throughout the CENTCOM theater. In fiscal year (FY) 2007, Internet cafes have grown to approximately 400, with an identified requirement for an additional 250 in FY 2008. The cost of bandwidth to support 650 Internet cafes is $27.4 million with an addition $20.3 million for equipment spares, supporting manpower and other documented costs for a total of $47.8 million. Within the CENTCOM theater, the Army Air Force Exchange Service provides in-room Internet service at Camp Liberty, Camp Stryker, and Camp Cropper, Iraq with 8,000 active subscribers. There is a 50-workstation Internet café at Al Taqaddum, Iraq servicing approximately 5,700 individuals. High-speed Internet service is also available inside the military barracks in Bagram and Kandahar, Afghanistan, servicing approximately 21,000 users. Deployed personnel routinely use these Internet cafes and other wired and wireless networks in various locations throughout Iraq to visit sites like *myspace.com* and *youtube.com*. The DoD's Space and Naval Warfare Command oversees a contract consisting of some 350 "large" and "small" low cost Internet cafes throughout the CENTCOM region, with the capacity to accommodate 200,000 personnel (Appendix C).

(U) Finally, the Army Knowledge Online and Defense Knowledge Online network is available to military members and their families, providing a rich information-sharing environment including e-mail; file sharing of pictures; videos and documents; discussion forums or blogging; instant messaging; chat rooms; and video messaging.

4.3 Commercial Considerations (U)

(U) It should be noted that prior to the DoD web-filtering action, members of DoD consulted with representatives from both *myspace.com* and *youtube.com* to weigh technical aspects of the filtering action. While discussions were engaging and mutually beneficial, it was ultimately the position of DoD that technical accommodations could not be worked to preclude the necessity for near-term IP address filtering.

5. Implementation of Web Filtering Action (U)

(U) The web-filtering action was conducted consistent with the procedures for downward-directed, enterprise-wide configuration changes within the DoD. It was extensively coordinated among GIG stakeholders (network operations centers, Defense activities and command staffs) to ensure that exceptions were identified and addressed well in advance of the action. The result was a Department-wide awareness and acceptance of the action prior to its implementation (detailed coordination timeline at Appendix D).

(U) The filtering action was directed by the Joint Task Force Global Network Operations (JTF-GNO), the DoD's operational arm in implementing GIG-wide modifications and security enhancements. In its Operational Directive Message (ODM) 059-07 ("IAP Access Control List (ACL) Security Filter Update"), the JTF-GNO indicated the following recreational web sites would be access-controlled (on or about 16 May 2007) at all DoD IAPs: *youtube.com; 1.fm; pandora.com; photobucket.com; myspace.com; live365.com; hi5.com; metacafe.com; mtv.com; ifilm.com; blackplanet.com; stupidvideos.com;* and *filecabi.com.*

6. Measurable Effects of the Filtering (U)

(U) DoD's filtering action demonstrated immediate, measurable effects at the IAPs. Following the implementation of the ODM, engineers noted some 140Mbps of bandwidth freed for DoD operations. Notionally, as a point of reference, this was roughly the amount required to support 70 unmanned aerial vehicle video feeds. As to the question of what operations actually were cleared to occur in the wake of the freed network space, the GIG is not calibrated to measure the immediate tradeoff between reduced recreational web browsing and the resultant increase in "official" mission-related operations. Rather, the DoD sees its overarching responsibility to ensure the unfettered availability of bandwidth. Therefore, the operational results of web filtering will not be immediately evident, but will require ongoing analysis, anecdotal evidence, and scrutiny of other lagging indicators that might otherwise reveal the ways in which freed capacity is being used.

(U) In terms of negative effects on the GIG, the web-filtering event was negligible. Isolated incidents of "collateral damage" were contained by reauthorizing access to those who suffered incidental loss of GIG service. For example, *filecabi.com* was removed from the list because the action also blocked several DoD support activities with a legitimate requirement for access to the GIG. Additionally, it was discovered soon after implementation that *mtv.com* and *ifilm.com* were not capable of being filtered by traditional IP address targeting due to the configuration of their content hosting server.

(U) From a security perspective, there were no indicators to suggest that a threat or hostile act was suddenly interrupted as a result of the filtering. Again, the security aspect of this action must be viewed in the context of a strategic, forward-looking defense measure that seeks to reduce unnecessary exposure rather than thwart hostile activities in progress (although the latter cannot be categorically ruled out as a possible effect of this action).

(U) Although the filtering action resulted in public scrutiny and concern for deployed personnel, it was largely transparent to this user community, given the availability of commercial Internet options. The decision to filter sites was based on considerations other than content, and did not impinge upon any First Amendment rights American citizens and uniformed Service members enjoy. DoD is working to give alternative access to such sites by funding and support of the Internet cafes.

7. Personal Internet Communications (U)

(U) Personal Internet communications, including e-mail, web logs (BLOGs), video web logs (VLOGs), wireless text messaging, and other emerging Internet based media are a convenient means for Service members to interact. However, these Internet communication media are also open and accessible to the enemies of the United States. Our enemies are increasingly skillful at using Internet media to further their agendas while undermining U.S. and allied efforts. DoD information security policies seek to protect military security while promoting free expression. Recently, the Army released an updated Operations Security (OPSEC) policy, Army Regulation 530-1, which requires Army personnel to consult with a supervisor and their OPSEC officer before posting information in a public forum. This includes letters, emails, web site postings, and BLOG and VLOG postings among other types of

information. The intent is not to impede Army members from blogging while in theater, rather to protect sensitive military information that could expose capabilities, vulnerabilities, techniques, or scheduling. However, given recent misconceptions surrounding the intent of the policy, the Army is currently developing clarifying guidance to this new policy. In addition, the DoD plans to issue guidance on Personal Internet Communication. Overall, these policies are needed to adapt to technological communications advancements and the ease of accessibility, instantaneous nature and global reach of these easy forms of communications.

8. Policies and Procedures on Releasing Official Information (U)

(U) The DoD must protect sensitive information and policies for such protection are an integral part of the Department's overall strategy. In this regard, long-standing policies concerning public release of DoD information include DoD Directive 5230.9 "Clearance of DoD Information for Public Release" and DoD Instruction 5230.29, "Security and Policy Review of DoD Information for Public Release." Under these regulations any official DoD information intended for public release that pertains to military matters, national security issues, or subjects of significant concern to the Department of Defense shall be reviewed for clearance by appropriate security review and public affairs offices prior to release. Official DoD information includes "all information that is in the custody and control of the DoD, relates to information in the custody and control of the Department, or was acquired by DoD employees as part of their official duties or because of their official status within the Department." Information to be posted to social networking sites about environmental (living and operating) conditions, operation success/shortcoming, schedules and problems in Iraq, Afghanistan and other forward operating areas meets this definition.

(U) The DoD attempts to afford soldiers every opportunity to connect with family and friends and to exercise their rights to free speech. For example, DoD policy provides that DoD personnel, while acting in a private capacity and not in connection with their official duties, have the right to prepare information for public release through non-DoD forums or media. Such activity is authorized if:

(1) (U) No laws or regulations are violated;
(2) (U) Ethical standards and compliance with DoD Directive 5500.7 "Standards of Conduct" and DoD 5500.7-R "Joint Ethics Regulations" are maintained;
(3) (U) The preparation activities are not done during normal duty hours or with the use of DoD facilities, property, or personnel except as authorized by the "Standards of Conduct" and "Joint Ethics Regulations";
(4) (U) The author does not use official DoD information generally not available to the public and which would not be released under the DoD 5400.7-R "DoD Freedom of Information Act Program."

(U) In addition, the DoD has issued several memoranda related to the vulnerability and protection of information on the web:

- (U) Assistant Secretary of Defense (C3I) Memo, "Web Site Administration Policies and Procedures," November 25, 1998 (with corrections from January 11, 2002);
- (U) Secretary of Defense Memo, "Information Security/Website Alert," August 6, 2006.

(U) Also, the Department's information assurance and information security program policies govern the protection of both classified and sensitive but unclassified information within the Department. These include:

- (U) DoD Directive 8500.01E, "Information Assurance," October 24, 2002.
- (U) DoD Directive 5200.1, "DoD Information Security Program," December 13, 1996.
- (U) DoD Regulation 5200.1-R, "Information Security Program," January 14, 1997.
- (U) DoD Instruction 8500.2, "Information Assurance Implementation," February 6, 2003.

9. Web Site Administration and the Content of Publicly Accessible Web Sites (U)

(U) A major concern for the Department is the need to provide information that is accessible and current to the public. The Internet provides DoD with a powerful tool to convey suitable information quickly and efficiently on a broad range of topics relating to its activities, objectives, policies and programs. The American democratic process rests on the right of our citizens to know what government is doing, and the corresponding ability to judge its performance. Access to information by the public through the Internet is an important component of this right. Nevertheless, careful examination of the potential consequences of placing information on the Internet must be undertaken before it is made available.

(U) The DoD has a number of information policies governing information dissemination, several of them related to information in electronic format; many related to national security concerns and clearance requirements; and several pertaining to the management and availability of records in printed or electronic form. The core policy related to the dissemination of government information to the public is the "Principles of Information" in DoD Directive 5122.5, "Assistant Secretary of Defense for Public Affairs." Generally, DoD guidance requires that "information be made fully available unless its release is precluded by national security constraints or statutory mandates or exceptions. Information should be withheld when disclosure would adversely affect national security, threaten the safety or privacy of government personnel or their families, violate personal privacy, or be contrary to law.

(U) The Office of the Assistant Secretary of Defense for Public Affairs operates and maintains Defense Link as the primary gateway to DoD data on the Internet. DoD sites must register with DefenseLINK or their Service component. The public affairs office sets up a central web site registration system that meets the requirements for the Government Information Locator Service (GILS), an initiative mandated by the Office of Management and Budget to inform the public where data can be found. Defense Agencies and the Services also create central registration systems that meet GILS requirements and are integrated with Defense Link.

(U) Obviously, establishing web sites goes beyond general public affairs considerations. Comprehensive risk management procedures at the lowest levels must ensure that the mission benefits gained by using the Internet are carefully balanced against potential security and privacy risks by having aggregated DoD information more readily accessible to a worldwide audience. When combined with information from other sources, information improperly obtained from vulnerable DoD systems may place DoD personnel at risk. Given the increasing dependence of our national and economic security upon the information infrastructure, it is essential that commanders and other organizational heads review organizational information connectivity and

content to ensure good OPSEC procedures are being applied within their organizations. The individual Services and Agencies have issued policies to meet their needs, consistent with DoD-wide guidance. Web guidance issued and implemented by individual Services and Agencies can be accessed at http://www.defenselink.mil/webmasters/.

10. Summary and Way Ahead (U)

(U) Recreational web browsing cannot be left unchecked in DoD systems and available to be exploited by hostile actors. The sites affected by this filtering action will serve as an important baseline for consideration of the need for future recreational IP restrictions, which will come only with further engineering analysis and Department-wide coordination.

(U) As DoD continues to assess its network vulnerabilities, more filtering may be required to tamp the ever-increasing demand for bandwidth and to mitigate the security vulnerabilities introduced by certain web technologies and entities. Future infrastructure enhancements may provide the DoD with a more granular and more efficient means of filtering web sites that do not serve an operational purpose, but until this can be implemented to the satisfaction of engineers and security experts, IP address filtering will remain the method of choice.

(U) Web filtering is but one mechanism the DoD will employ in its attempt to avoid GIG saturation. Infrastructure investments will continue commensurate with the increase in network-dependent applications, and resource decisions will be made to support operational requirements.

Appendix A

DoD Policy (U)

DoD Report to Senate Armed Services Committee on DoD Personnel Access to the Internet

(U) Unified Command Plan 2006 (See USSTRATCOM Authorities)

(U) Secretary of Defense Memorandum, June 18, 2004, "Assignment and Delegation of Authority to Director, Defense Information Systems Agency (DISA)"

(U) DOD 5500.7-R, Change 6, March 23, 2006, "Joint Ethics Regulation"

(U) DOD Instruction 5200.40, December 30, 1997, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)"

(U) DOD Directive 8000.01, February 27, 2002, "Management of DoD Information Resources and Information Technology" (Certified Current as of April 23, 2007)

(U) DOD Directive 8100.01, September 19, 2002, "Global Information Grid (GIG) Overarching Policy"

(U) DOD Directive 8500.01E, October 24, 2002, "Information Assurance (IA)" (Certified Current as of April 23, 2007)

(U) DOD Instruction 8500.2, February 6, 2003, "Information Assurance (IA) Implementation"

(U) DOD Directive O-8530.1, January 8, 2001, "Computer Network Defense (CND)"

(U) DOD Instruction O-8530.2, March 9, 2001, "Support to Computer Network Defense (CND)"

(U) DOD Instruction 8552.01, October 23, 2006, "Use of Mobile Code Technologies in DoD Information Systems"

(U) CJCSI 6211.02 Series, July 31, 2003, "Defense Information System Network (DISN): Policy, Responsibilities and Processes" (Certified Current as of Aug 30, 2006)

(U) CJCSI 6510.01D, June 15, 2004, "Information Assurance (IA) and Computer Network Defense (CND)"

(U) CJCSM 6510.01 Series, Change 3 March 8, 2006, "Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND)" (Certified current as of Mar 14, 2007)

(U) USCENTCOM Regulation No. 380-8, "Automation Information Systems (AIS) Security Program," August 20, 2001

Appendix B

Source Documents (U)

DoD Report to Senate Armed Services Committee on DoD Personnel Access to the Internet

1. **PRE-DECISIONAL SOURCES (U)**

A. DISA and JTF-GNO Analysis (U)

(U) Carnegie Mellon Software Engineering Institute, "NIPRNet Bandwidth Study" July 2006

(U) DISA "Internet Traffic Survey: October, 2006" 13 November 2006

(U) JTF-GNO WARNORD# 07-003, "Blocking Recreational Traffic at the Internet Access Points (IAP)," 6 February 2007

(U) JTF-GNO Operational Directive Message (ODM) # 059-07, "Internet Access Point (IAP) Access Control List (ACL)/Security Filter Update," 15 May 2007

B. Industry Reports (U)

(U) McAfee Avert Labs Unveils Predictions for Top Ten Security Threats in 2007 as Hacking Comes of Age (http://www.mcafee.com/us/about/press/corporate/2006/20061129_080000_f.html)

(U) Sophos Security Threat Report 2007 (http://www.sophos.com/pressoffice/news/articles/2007/01/secrep2007.html)

(U) Symantec Internet Security Threat Report, Trends for January 06–June 06, Volume X, Published, September 2006 http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_symantec_internet_security_threat_report_x_09_2006.en-us.pdf

C. Open Press Articles (U)

(U) IT News, "Cyber-criminals target MySpace users," Clement James, 6 October 2006, http://www.itnews.com.au/News/NewsStory.aspx?story=37899

(U) Web Sense, "Fraudulent You Tube video on MySpace installing Zango Cash," 06 November 2006, http://www.websense.com/securitylabs/alerts/alert.php?AlertID=689

(U) Fortinet, "Top 10 High-risk Security Threats for March 2007 announced by Fortinet," March 2007, http://www.techshout.com/internet/2007/10/top-10-high-risk-security-threats-for-march-2007-announced-by-fortinet/

(U) BBC News, "Virus writers target web videos," Mark Ward, 31 October 2006, http://news.bbc.co.uk/go/pr/fr/-/2/hi/technology/6100016.stm

(U) Web Sense, "MySpace XSS QuickTime Worm," 01 December 2006, http://www.websense.com/securitylabs/alerts/alert.php?AlertID=708

(U) PC Magazine, "MySpace Users Get MyMalware," Natali T.Del Conte, 21 July 2006, http://www.pcmag.com/article2/0,1895,1992926,00.asp

(U) Washington Post, "Hacked Ad Seen on MySpace Served Spyware to a Million," Brian Krebs, 19 July 2006, http://blog.washingtonpost.com/securityfix/2006/07/myspace_ad_served_adware_to_mo.html

2. SUBSEQUENT (POST-DECISIONAL) SUPPORTING MATERIAL (U)

A. Federal Government Reports (U)

(U) GAO Report # GAO-07-751T, "Information Security, Persistent Weaknesses Highlight Need for Further Improvement," April 19, 2007

B. DoD Correspondence (U)

(U) ASD(NII), John G. Grimes, Memo to the Honorable Edward J. Markey U.S. House of Representatives

C. Open Press Articles (U)

(U) Government Computer News, "Whose Tube? Not the DOD's," Patience Wait, May 21, 2007, http://www.gcn.com/print/26_11/44292-1.html

(U) Network World, "Zlob Malware Hijacks YouTube," John E. Dunn, June 6, 2007, http://www.networkworld.com/news/2007/062107-zlob-malware-hijacks.html

(U) Network World, "How MySpace is Hurting Your Network; Social Networking Sites Drives up DNS Traffic Bandwidth," Carolyn Duffy Marsan, Network World, June 22, 2007, http://www.networkworld.com/news/2007/062207-myspace.html?page=1

(U) Government Executive, "Defense Official Responds to Critics of Decision to Ban Popular Web Sites," Bob Brewin, July 2, 2007, http://www.govexec.com/dailyfed/0707/070207mag1.htm

Appendix C

DoD Cyber Café Contract (U)

DoD Report to Senate Armed Services Committee on Personnel Access to the Internet

HEADQUARTERS
MULTI-NATIONAL CORPS - IRAQ
BAGHDAD, IRAQ
APO AE 09342

MNC-I Policy Letter C6-11

FICI-CE-I

JAN 2 9 2007

MEMORANDUM FOR DISTRIBUTION

SUBJECT: MWRNET Internet Cafe Policy

1. **PURPOSE**. This memorandum defines the MNC-I policy for the life cycle of the Morale, Welfare and Recreation Network (MWRNET) Internet Cafes. This policy covers determining requirements, requesting Cafés, operation and maintenance, and transfer and disposal of MWRNET Internet Cafés.

2. **BACKGROUND**. In November 2003, MNC-I C6 established an agreement with Space and Naval Warfare Systems (SPAWAR), a DoD Naval Engineering Command, to provide Internet Cafés for units operating in the Iraqi Theater of Operations (ITO). The agreement calls for SPAWAR to procure equipment, train Café operators and provide regional technical support for the Internet Cafés. MWRNET facilities are sponsored by military units and are established at bases based on the population density of authorized users.

3. **POLICY**:

a. **Terms and Definitions**. As used in this document, the following terms have these specific meanings:

1. Unit – the military unit that requests a MWRNET Internet Café, operates the Café, and carries the Café equipment on their Theater Provided Equipment (TPE) Property Book.

2. Installation Commander – the senior commander assigned responsibility over a particular camp, post, Forward Operating Base (FOB) or Contingency Operating Base (COB).

3. Mayor Cell – the agent responsible for land management at a camp, post, FOB or COB.

4. Contracting Officer's Technical Representative (COTR) – The MNC-I C6 is the COTR for the MWRNET project and provides oversight. The COTR ensures the Cafés are properly managed in the best interest of the users and the government.

5. Contracting Officer Representative (COR) – SPAWAR is the COR and assists in the technical monitoring or administration of the contract. However, the COR may not delegate the authority to make any commitments or changes that affect price, quality, quantity, delivery or other terms and conditions of the contract.

6. Large Café – Café consisting of 20 computers, 8 Voice over Internet Protocol (VoIP) telephones, 3 Web Cams and support equipment required for satellite uplink providing connection to the Network Operating Center (NOC).

7. Small Café – Café consisting of 5 computers, 3 VoIP phones, 1 Web Cam and support equipment required for satellite uplink providing connection to the NOC.

8. SPAWAR NOC- NOC (Network Operations Center) is central office for all SPAWAR operations for the IRAQ AOR.

b. **Determining Requirements**. In order to establish a MWRNET Internet Café, the following minimum requirements must be met:

1. Café distribution. One Large Café supports 1,000 US government and civilian Common Access Card (CAC) holders per geographic location. One Small Café supports 500 CAC holders or less. Special consideration will be given based on remoteness, accessibility, type of facility and services available at that location. The Installation Commander will determine if a new Café is necessary based on population density of the installation. The Installation Commander will determine if the need for a Café can be mitigated by relocating an existing Café within his Area of Operations (AOR).

2. Café location. The requesting unit must coordinate with the Mayor Cell and the Installation Commander to determine optimal locations of all Internet Cafés within each geographic location. The location must promote maximum use and facilitate access by all valid CAC holders. Access and use by Third-Country Nationals (TCNs) is at the discretion of the Installation Commander. AAFES TCNs are authorized access to all MWRNET Internet Cafes. Cafés will never be placed in an area where admittance requires special access badging in addition to the CAC.

c. **Requesting a Café**.

1. Requests for procurement of MWRNET Internet Cafés will be submitted to the MNC-I C6 Validation Board (C6VB) by individual units. Requests will be in the form of a standard Validation Board packet, available on the MNC-I C6 SIPR portal page at [http://spsm.iraq.centcom.smil.mil/C19/C4/C6%20Validation%20Board/default.aspx].

2. Additional required supporting documentation includes a memorandum from the Installation Commander documenting the CAC holder current population of the installation and the number of Cafés currently providing service in that AOR. Deviations from the defined distribution (section (B)(1) above), if any, must be justified in this memorandum.

3. The C6VB forwards validated packets to the MNC-I C8 for funding approval and prioritization. Upon MNC-I C8 approval, the unit will be notified via the Validation Board tracker on the MNC-I SIPR portal page at [http://spsm.iraq.centcom.smil.mil/C19/C4/C6%20Validation%20Board/default.aspx]. All costs for the initial installation and first year of service are borne by the requesting unit. The unit is responsible for completing DD Form 448: Military Interdepartmental Purchase Request (MIPR).

authorizing transfer of funds to SPAWAR. The unit will provide a copy of the MIPR to the MNC-I C6 MWRNET COTR.

4. The unit will coordinate details for delivery and installation directly with the SPAWAR NOC. This includes:

a. The unit will assign a Project Officer as the primary POC for the installation of the new Café. SPAWAR will assign a technician to the primary POC for the installation of the new Café.

b. As soon as the Café location is finalized, the unit POC must provide the exact location (latitude and longitude) to the SPAWAR POC in order to configure the satellite connection.

c. SPAWAR is responsible for shipping all equipment from CONUS to a SPAWAR Supply Point in the ITO. The unit is responsible for coordinating transportation of the MWRNET Internet Café equipment from the SPAWAR Supply Point to the final destination. SPAWAR will provide the unit details (dates, number of pallets, etc.). The unit must complete all movement requests to have the equipment shipped within theater, or must pick up the equipment themselves.

d. The unit is responsible for the initial physical installation and all non-technical upgrades as they relate to the physical structure and support of the Café, including: Panduit, conduit, tables, chairs and privacy phone booths.

e. The unit ensures that all installed equipment remains within 100 feet of the black box and that the satellite dish remains within 150 feet of the black box. SPAWAR will provide the necessary LAN cabling and cable from the black box to the satellite dish.

d. Café Operation and Maintenance.

1. Unit Responsibilities.

a. The requesting unit, or the unit that assumes responsibility of a Café, is primarily responsible for the operations and Operator Level maintenance of their Café. The unit must assign two personnel to perform daily operation and maintenance of their Café. These personnel should have at least three months remaining on their tour and should be comfortable working with computers. They will receive training as detailed in (4)(e) below. The unit will ensure these personnel are available for training.

b. Inventory Control. All MWRNET equipment is Theater Provided Equipment (TPE) and must be accounted for on the unit's TPE Property Book. The unit is responsible for

conducting regular inventories IAW AR 735-5 (or equivalent Service regulation) of MWRNET equipment and initiating an investigation for any equipment determined missing or damaged. No missing or damaged equipment will be replaced unless accounted for on a DA Form 1659, Report of Survey to Financial Liability Investigation of Property Loss (or equivalent Service form). The MNC-I C6 MWRNET COTR is the point of contact for requests to replace missing or damaged equipment.

c. Non-standard Equipment. No additional equipment whatsoever may be connected to the MWRNET without written approval provided through the MNC-I C6 MWRNET COTR. Non-authorized equipment slows down and disrupts the network. Prohibited items include, but are not limited to: personal computing equipment, switches, routers, hubs or cabling that is not part of the original package. Requests for installation and use of non-standard equipment is strongly discouraged and will be considered on a case-by-case basis per section F. *Waivers*.

d. Repairs. Equipment problems must be reported to the SPAWAR NOC IAW the MWRNET Escalation Policy. The unit should request a trouble ticket number in order to track the status of the repair. SPAWAR will attempt to repair the equipment on site. However, if equipment must be shipped, the unit must make arrangements to ship any broken equipment from the installation to the nearest SPAWAR Supply Point and replacements from the SPAWAR Supply Point to the installation.

e. Maintenance. The unit is responsible for Operator Level and Preventative Maintenance and must perform all maintenance as described in the Turnover and Maintenance SOP. The unit is responsible for completing and posting Equipment and Maintenance worksheets (DA Form 2404).

f. Acceptable Use. MWRNET Internet Cafés, regardless of location, are paid for with MWR funds and will only be used for recreational purposes. No official business may be conducted on any MWRNET computer. Converting a MWRNET Internet Café computer to a computer used for mission operational use is explicitly prohibited. No MWRNET Internet Café equipment may be removed, relocated or altered FOR ANY PURPOSE without written authorization from the MNC-I C6 COTR.

g. Hours of Operation. Hours of operation are at the discretion of the Unit Commander. All Cafés are encouraged to be open 24 hours a day, seven days a week. However, local conditions may dictate otherwise. Cafés are authorized to stand-down for up to 2 hours per day in order to conduct scheduled maintenance and servicing.

h. A copy of the following documents must be posted at each Café:

1. Standard Operating Procedures.

a. MNC-I MWRNET Internet Café Policy (this Policy Letter)

b. MWRNET Escalation Policy
[https://www.mnci.iraq.centcom.mil/C5/MWRNET/Document%20Library/MWR_NOC%20Escalation%20Policy%20signed.pdf]

c. Turnover and Maintenance SOP
[https://www.mnci.iraq.centcom.mil/C5/MWRNET/Document%20Library/SPAWAR%20Turnover%20and%20Maintenance%20SOP.doc]

d. Equipment and Maintenance Worksheet (DA Form 2404)

2. Installation Commander Responsibilities.

a. Responsible for placement of all Cafés within their AOR.

b. Ensuring units operating Cafés are performing maintenance and conducting periodic inventories.

c. Ensuring all Cafés in their AOR remain accessible to all CAC holders.

3. Mayor Cell Responsibilities.

a. For all Cafes located within a MWR Facility, including those operated by KBR, the Mayor Cell assumes all responsibilities identified under section 3.D.(1) *Unit Responsibilities*. MWRNET equipment located in MWR facilities must be accounted for on the Installation Property Book (IPB).

b. The Mayor Cell must assign personnel to perform the Operator Level and Preventative Maintenance on all Cafés which are currently operated by KBR.

4. SPAWAR Responsibilities.

a. SPAWAR NOC is responsible for Intermediate Level and Depot Level maintenance on all MWRNET equipment as defined in the Turnover and Maintenance SOP. This includes replacement of assemblies and sub-assemblies such as keyboards, mice, web-cams, and UPSs.

b. SPAWAR technical assistance is the only authorized service (other than Operator Level maintenance and Preventative Maintenance conducted by personnel in accordance with the Turnover and Maintenance SOP) for MWRNET Internet Cafés. SPAWAR is not responsible for repairs to equipment damaged as a result of maintenance conducted by unauthorized personnel.

c. SPAWAR is not authorized to conduct repairs on non-MWRNET equipment.

d. SPAWAR will periodically conduct inventories of the MWRNET Internet Cafes during site visits and provide reports back to the MNC-I C6 MWRNET COTR.

e. Training. Concurrent with a new Café being issued, within 30 days after a RIP/TOA, or as requested by a unit, SPAWAR will provide training to the personnel assigned to the operation and maintenance of the Café. The training will be conducted either centrally at the SPAWAR facility at LSA Anaconda or at the unit. This training will consist of: Café setup and operation, Operator Level and Preventative maintenance, and troubleshooting.

5. MNC-I C6 Responsibilities

a. MNC-I C6 MWRNET COTR is responsible for the administration and technical advise and analysis related to the overall management of the MWRNET within the ITO.

b. MNC-I C6 MWRNET COTR formulates and coordinates maintenance requirements via the Turnover and Maintenance SOP at the direction of the contracting officer.

c. **Temporary Suspension of Service.** Commanders at any level may temporarily suspend service in their AOR in order to prevent the release of sensitive information such as operational casualties, pending next-of-kin notification, statements of operational climate, and local media reports of current events. The Commander should alert the SPAWAR NOC both prior to disconnecting their Café and after reconnecting their Café. Failure to coordinate with the NOC may result in the Café not functioning properly after reconnection.

f. **Café Transfer and Disposal**

1. No Café may be relocated within an installation or between installations without prior coordination with MNC-I C6 COTR and SPAWAR NOC. The Installation Commander, in coordination with the Mayor Cell, is the approval authority for relocations within their AOR.

2. Base Realignment and Closure (BRAC). MWRNET Internet Cafés affected by BRAC will follow the procedures detailed in the Base Closure SOP.

3. During a Relief in Place and Transition of Authority (RIP/TOA) the Installation Commander will ensure that the departing unit transfers all equipment to the incoming unit as Theater Provided Equipment (TPE) on the units' property books. Any equipment found to be missing must be accounted for on a DA Form 1659, Report of Survey to Financial Liability Investigation of Property Loss (or equivalent Service form).

g. **Waivers.** Requests for Waiver to any section of this policy must be submitted in writing to the MNC-I C6 MWRNET COTR. Waivers will be granted on a case-by-case basis. Units must provide well supported justification.

h. **Non-compliance.** Any unit that is found to be in non-compliance with this policy may have their MWRNET Internet Café disconnected from the MWRNET until they come into compliance. The Unit Commander, Installation Commander or MNC-I ACoS C6 is authorized to terminate service of any Café within their area of control. Repeated violations may result in the removal of the MWRNET Internet Café.

4. **Point of Contact Information:**

a. MNC-I C6 MWRNET Project Manager: MAJ Andre Burks, DSN: 318-822-4021, email: [illegible]@iraq.centcom.mil

b. SPAWAR Project Engineer: Jim Clarkson, DSN: 318-443-6148 (LSA Anaconda), 314-421-2911 (Stuttgart, GE), email: [illegible]@spawar.navy.mil

c. SPAWAR NOC (Stuttgart, GE): DSN: 318-443-6198 or 314-421-2525, email: [illegible] or [illegible], COMM 973-735-1860 (this number may be called from any MWRNET Internet Café telephone at no charge)

RAYMOND T. ODIERNO
Lieutenant General, USA
Commanding

DISTRIBUTION:
IAW MNC-I (S/S) Form 1855 A

Appendix D

Timeline of Events (U)

DoD Report to Senate Armed Services Committee on DoD Personnel Access to the Internet

Date	Event
7 Mar 05	(U) DISA begins regularly monitoring and reporting top Internet domains sending traffic to DoD
13 Nov 06	(U) DISA releases quarterly Internet Traffic survey, including list of top domains that is later used to influence blocking choices.
12 Dec 06 – 5 Feb 07	(U) JTF-GNO coordinates proposal with OSD, the Joint Staff (JCS), Combatant Commands (COCOM), Military Services, and DoD Agencies.
6 Feb 07	(U) JTF-GNO Warning Order (WARNORD) 07-003 "Blocking Recreational Traffic at the Internet Access Points (IAP)" released to OSD, the Joint Staff, Combatant Commands, Military Services, and DoD Agencies.
22 Feb 07	(U) Commander, JTF-GNO briefs COCOM J6s at Joint Staff J6 Winter Conference.
28 Feb 07	(U) JTF-GNO receives comments from OSD, JCS, COCOMs and Agencies. JTF-GNO establishes list of exceptions based on inputs.
22 Mar 07	(U) JTF-GNO hosts discussions with MySpace and YouTube regarding website security postures.
27 Apr 07	(U) Commander, JTF-GNO completes resolution of all issues.
30 Apr 07	(U) Commander, US Strategic Command (USSTRATCOM) approves proposed blocking of recreational web sites.
15 May 07	(U) JTF-GNO releases Operational Directive Memorandum (ODM) 059-07 "Internet Access Points Access Control List Security Filter Update," which mandates blocking of recreational web sites, with compliance by 16 May 07.
17 May 07	(U) Vice Commander, JTF-GNO, participates in DoD press conference with media.
24 May 07	(U) Vice Commander, JTF-GNO, hosts teleconference with leadership or representatives of 13 websites
25 May 07	(U) Commander, JTF-GNO briefs Senior DoD and COCOM leaders on status of recreational web blocking
29 May 07	(U) Vice Commander, JTF-GNO, briefs status of recreational web blocking to the Deputy Assistant to the President, and Deputy National Security Advisor for Strategic Communications & Global Outreach