Projected Impacts of the Internet Protocol version 6 (IPv6) on the USN and USMC Enterprise

Michael P. Brig
SPAWAR Systems Center Charleston
PO 190022
North Charleston, SC 29419
843-218-4675
brigm@spawar.navy.mil

The views and opinions expressed in this paper are those of the author and do not necessarily reflect those of the US Navy or Marine Corp.

ABSTRACT*: The emerging Internet Protocol version 6 (IPv6) standard should profoundly impact the US Navy (USN) & Marine Corp (USMC) Network Centric Enterprise. The IPv6 protocol enables the realization of new Network Centric Warfare (NCW) concepts and doctrine while improving the scalability, robustness, security, and manageability of USN & USMC communications. These improvements may be realized at a substantial cost if the transition from the current Internet Protocol version 4 (IPv4) standard is not managed, resourced, and coordinated properly. The scope of the transition should encompass nearly every program and community within the USN and USMC enterprise. A list of projected impacts to the USN and USMC enterprise due to the deployment of the IPv6 protocol are provided. As with any new technology, the impacts are both positive and negative. Examination of the list demonstrates a clear and compelling need for a comprehensive USN and USMC enterprise IPv6 transition strategy and program to maximize the benefits and minimize the negative impacts and costs to the fleet.*

1. Introduction

IPv6 is the next generation end-to-end protocol of the Internet. IPv6 has become necessary due to fundamental limitations in the current IPv4 protocol standard which render IPv4 incapable of meeting the long-term requirements of the commercial Internet. IPv6 was designed to overcome these limitations by expanding available address space, improving routing, providing end-to-end security, facilitating mobile communications, providing new enhancements to quality of service, and easing system management burdens.

While the timing and speed of a commercial move to IPv6 is uncertain, it is expected to gradually replace IPv4 over the next several years. The tremendous capital investments in IPv4 technology by users worldwide as well as the USN and USMC enterprise will likely result in an extended transition period where both protocols coexist. At some time in the future, the USN and USMC enterprise should be prepared to retire the IPv4

standard in concert with the entire joint Department of Defense (DoD) community.

2. Background

The US military began designing the IPv4 protocol in the early 1970s as part of the ARPANET program and the Defense Communications Standardization Effort (DCSE). In 1978, the Office of the Secretary of Defense (OSD) mandated the use of the IPv4 protocol for all "host-to-host" data exchange enabling IPv4 to become the mechanism for the military to create integrated verses stovepiped communications. Following orders, the military promptly built nearly all its communications and software upon the IPv4 standard. For example, the Secret IP Router Network (SIPRNET), the Non-classified IP Router Network (NIPRNET), the Joint Worldwide Intelligence Communications System (JWICS), all connected systems, and most software are based upon the IPv4 standard.

IPv4 became a successful commercial standard beginning in the early 1990s as the Internet began a rapid process of commercialization and internationalization. Today the Internet consists of over 200 million computers in over 50 nations. Many critical commercial applications are based upon IPv4 such as Business-to-Business (B2B) and Business-to-Consumer (B2C) e-commerce as well as the World Wide Web (WWW) and the global email system. In addition, many (Internet Engineering Task Force) IETF standards have been found to be dependant upon the IPv4 protocol in one form or another. See IETF draft draft-ietf-ngtrans-ipv4survey-02.txt for further information.

In the past five to ten years, the military has made a determined effort to fully utilize Commercial-Off-The-Shelf (COTS) technology verses military developed technology. Military modernization has greatly benefited from the use of low-cost state-of-the-art COTS technology. Commercial products supporting IPv4 are inexpensive and are available nearly everywhere. The military has, for this and many other reasons; built IPv4 based COTS and Government-Off-The-Shelf (GOTS) hardware and software throughout its communications and the military establishment.
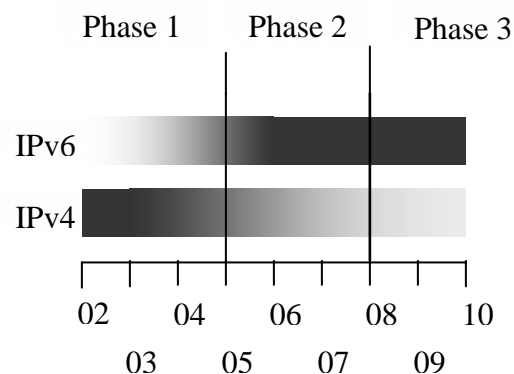
3. Timeframe

Figure 1. Potential USN and USMC Enterprise IPv6 Deployment Timeframe

The DoD transition to the IPv6 protocol is expected to consist of three distinct phases as shown in Figure 1. Phases are separated by transition events which, at this time, have no firm implementation dates. Phase 1 is the period of time IPv6 is an emerging standard while IPv4 is the mandatory standard end-to-end protocol of the DoD Joint Technical Architecture (JTA). The USN and USMC enterprise is currently in this stage of IPv6 deployment. Phase 2 is the period of time when both IPv4 and IPv6 should be mandatory standard end-to-end protocols of the JTA. Phase 3 is the period

of time IPv6 should be the sole standard end-to-end protocol of the JTA.

The transition events of Figure 1 will likely be event and resource driven. They will likely reflect fundamental changes in the JTA. The transition events could also reflect mandates from high-level management within the DoD such as the Assistant Secretary of Defense Office of the Secretary of Defense for Command, Control, Communications, and Intelligence (ASD C3I). The first transition event should initiate coordinated efforts to efficiently and effectively engineer the IPv6 protocol into USN and USMC enterprise communications. The second transition event should initiate coordinated efforts to retire the IPv4 protocol and IPv6 co-existence mechanisms from USN and USMC enterprise communications. The second transition event could well be significantly larger, costlier, and more complex than the first transition event. The impacts of the emerging IPv6 standard to the USN and USMC enterprise will; therefore, vary greatly with time.

DoD dependence on COTS technologies may be a key factor in determining when the transitions events described in Figure 1 will occur. As the transition progresses, greater numbers of dual stacked and IPv6 only products and services are expected to reach the commercial marketplace. Fewer IPv4 only products will likely come to market as the number of dual stacked products increase. This behavior has been demonstrated by the trends of the past four years. Eventually, IPv4 only products may not be widely available on the commercial market.

Industry projections for the timing of the transition from IPv4 to IPv6 are as undefined as that shown in Figure 1. Figure 2 shows the current Cisco Systems projected timeframe for IPv6 adoption. Note that Figure 2 does not include consideration for the retirement of IPv4. The IETF Request For Comments (RFCs) clearly state there should be a transition to IPv6 from IPv4 and the transition period should be kept as short as possible. A prolonged transition will likely be very costly and problematic. Most vendors are currently focusing on the first transition event and very few on the second transition event. The USN and USMC enterprise should consider vendor projections to properly plan for and budget for its transition to IPv6.
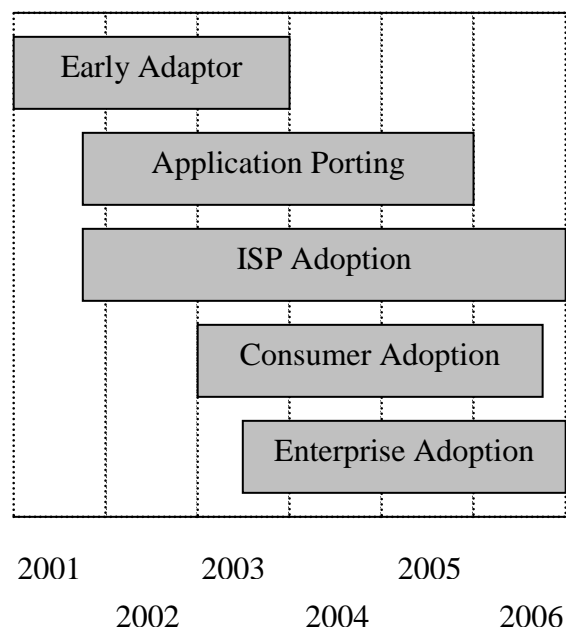

Figure 2. Cisco Systems Projected IPv6 Deployment Timeframe.

4. Current IPv6 Commercial Deployment

The global adoption of IPv6 is already underway and has been so since at least mid 1999 when the Regional Internet Registries (RIRs) began allocating production IPv6 address space to top-tier Internet Service Providers (ISPs). The RIRs are the American Registry for Internet Numbers (ARIN), Réseaux IP Européens (RIPE), and

the Asia Pacific Network Information Center (APNIC). Figure 4 shows the distribution of these top-tier production IPv6 ISPs from 40 nations. To date 214 top-tier ISPs have begun production deployment of IPv6 communications.
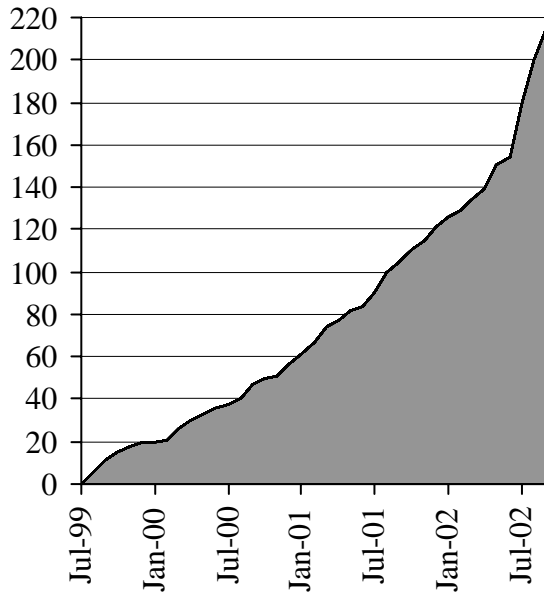

Figure 3. Growth in top-tier production IPv6 ISPs verses time.

Growth of the production IPv6 Internet verses time is illustrated in Figure 3. An average monthly growth of 5.6 top-tier IPv6 ISPs has occurred for the past 37 months. At this rate, 400 top-tier IPv6 ISPs can be expected by 2005. Some signs; for example Figure 5, indicate acceleration in this growth curve which could translate into a significantly greater numbers of top-tier IPv6 ISPs. Figure 3 only tracks the top-tier or backbone ISPs on the IPv6 Internet. Many smaller second and third-tier IPv6 ISPs already exist. Their number and growth trends are more difficult to track. It should be kept in mind that the IPv4 Internet can theoretically fit within the addressing resources of a single one of these top-tier production IPv6 ISPs.

#	Country	ISPs
1	Japan	46
2	US	24
3	Germany	18
4	S. Korea	14
5	UK	8
6	Netherlands	7
7	Europe	6
8	Austria	6
9	France	6
10	Mexico	5
11	Finland	5
12	Italy	5
13	Taiwan	5
14	Sweden	4
15	Norway	4
16	Poland	4
17	Australia	4
18	China	4
19	Canada	3
20	Portugal	3
21	Switzerland	3
22	Singapore	3
23	Thailand	3
24	Russia	2
25	Ireland	2
26	Spain	2
27	Lithuania	2
28	Denmark	2
29	Malaysia	2
30	Brazil	1
31	Luxembourg	1
32	Greece	1
33	Belgium	1
34	Czech	1
35	Hungary	1
36	Estonia	1
37	Cyprus	1
38	Yugoslavia	1
39	UAE	1
40	Papua New Guinea	1

Figure 4. Global Distribution of Top-Tier Production IPv6 ISPs as of September 2002.
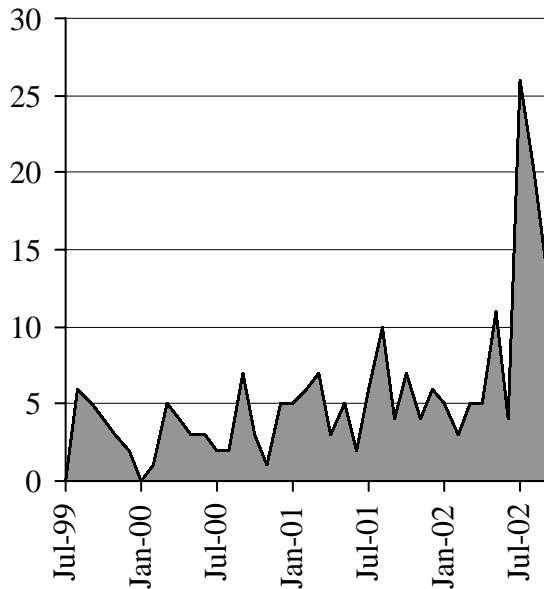
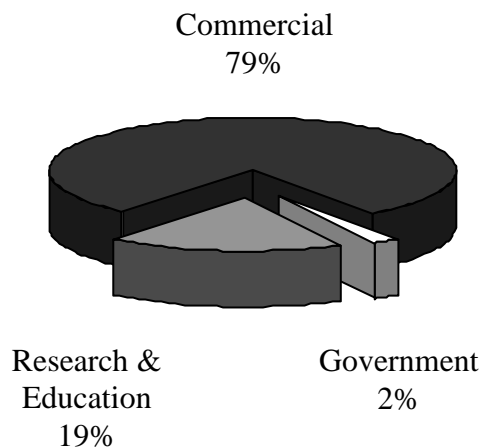Figure 5. Monthly Rate of Growth in top-tier production IPv6 ISPs.

Figure 6. Functional Distribution of Production IPv6 ISPs.

A pie chart of the functional distribution of top-tier IPv6 ISPs is shown in Figure 6. The largest sector of the production IPv6 Internet, 79%, consists of corporations and commercial ISPs. The total number of commercial IPv6 ISPs is currently 169. Research and education organizations constitute the next largest sector of the IPv6 Internet with 19% of the total IPv6 production Internet. The total number of

research and education IPv6 ISPs currently is 41. Government agencies constitute the smallest sector of the IPv6 Internet with only 2% of the total IPv6 production Internet. All four government IPv6 ISPs are currently administered by federal agencies of the United States including the Department of Energy, the Department of Defense, and NASA.
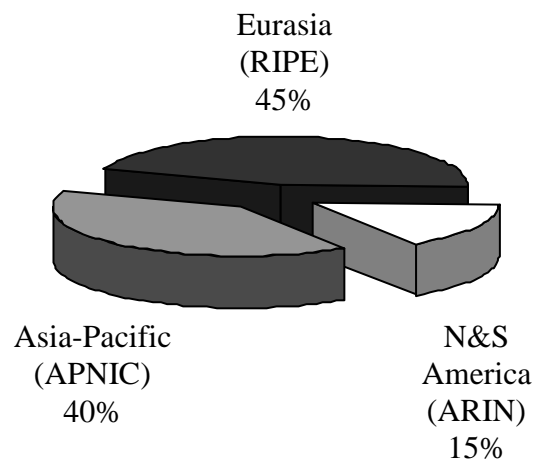

Figure 7. Geographic Distribution of Production IPv6 ISPs.

A pie chart of the geographic distribution of top-tier IPv6 ISPs is shown in Figure 7. Ninety-six IPv6 ISPs or 45% of the total originate in Eurasia. Eighty three IPv6 ISPs or 40% of the total originate in the Asia-Pacific. Thirty-three or 15% of the total originate from North and South America.

The 6BONE is a test IPv6 Internet that has been in existence since the beginning of 1996. There are 129 top-tier 6BONE IPv6 ISPs and many additional lower level IPv6 ISPs. The 6BONE ISPs are distributed in 56 nations around the world.

5. IPv6 Products

IPv6 has not yet been accepted as a universal and ubiquitous standard by all vendors but significant progress toward that

goal seems to be occurring. The broadest adoption of IPv6 has been in the open source software community. The [Apache Software Foundation](#) and [Mozilla.org](#) are two open source software development collaborations that produce application software in common use with the military. The [Internet Software Consortium](#) (ISC) is a not-for-profit corporation, which develops and maintains production quality open reference implementations of the Domain Name System (DNS) server software called BIND. BIND is widely used by the military on the NIPRNET, SIPRNET, and JWICS.

Most commercial Operating System (OS) platform and router vendors already have some level of support for IPv6 into their latest products and services. This group includes but is not limited to Microsoft, Cisco, Hewlett-Packard, Sun, IBM, Juniper, Hitachi, Yamaha, Nokia, and Apple. Others vendors have plans to incorporate IPv6 support or are in the midst of developing IPv6 support for their next generation products. This group includes but is not limited to Novell, Silicon Graphics, and Extreme Networks. Some vendors have no current plans to support the IPv6 protocol in the future. This group includes but is not limited to Oracle, Sybase, and SAP.

A number of COTS and open source applications have been ported to function with IPv6. Unfortunately, many of these application ports can only function with one or two OSs. There is no one OS that is capable of running all the IPv6 applications already ported.

6. Data Collection

Four means of data collection were utilized to draft this report. First, presentations were given at various USN and USMC conferences and meetings with feedback solicited from the audience. Second, USN and USMC web sites were searched for information pertaining to IPv6. Third, web sites from industry and standards organizations were searched for IPv6 information. Finally, information was collected through experimentation with the Defense Information Systems Network – Leading Edge Services IPv6 Pilot (DISN-LESv6) IPv6 pilot network.

The greatest volume of information and knowledge came from experimentation. Searches of commercial and standards organization web sites were also very useful. Very little data was collect from USN or USMC sources. This may be an indication of continuing lack of awareness of the IPv6 issue within the USN and USMC enterprise.

7. Projected impacts of IPv6 on the USN and USMC Enterprise

a. New network centric warfare concepts and doctrine possible with IPv6.

IPv6 will allow FORCENET to fully integrate sensors, networks, weapons, platforms, information, and people to provide agile, lethal, efficient combat power. IPv6's end-to-end (E2E) architecture and IPsec allow for the full exploitation of new devices, technologies, concepts, and doctrine. These are likely not realizable with the current IPv4 standard.

IPv6 is the new E2E protocol for the commercial Internet. IPv6 packets travel from source to destination mostly unaltered by intermediate devices. This E2E behavior or architecture is the same the IPv4 protocol originally possessed but which has been lost due to the widespread use of Network Address Translation (NAT) in the DoD. Applications function most efficiently with

the E2E architecture and have the least interoperability problems. Internet Protocol security (IPsec) also requires the E2E architecture to function properly.

With IPv6, every device can be a server and client simultaneously. In this context, a server refers to a device's ability to source information to the net and a client refers to a device's ability to pull information from the net. This is not the case with the current IPv4 protocol standard. Many devices in the USN and USMC enterprise already cannot serve information since they are behind NATs. Devices behind NATs do not have relatively constant addresses and domain names so they cannot effectively act as sources of information to the net.

b. IPv6 provides superior networking capabilities compared with IPv4.

IPv6 provides superior networking capabilities in a number of ways. IPv6 has a vastly greater number of useable addresses than IPv4 enabling the growth of USN and USMC communications to meet future requirements. Scalability is important since new devices are constantly being added to the communications of the USN and USMC enterprise and they should be able to interoperate fully with one another. In addition, during times of war and mobilization, new facilities, personal, and capabilities must be quickly added to the enterprise. Communications must likewise grow to connect these new entities with the rest of the enterprise.

IPv6 offers a more scaleable routing system than IPv4. The IPv6 Internet routing system is also more robust and responsive to change than the IPv4 Internet routing system. It is arguable that the IPv4 Internet's routing system has already reached its growth potential. Most backbone

providers today actively filter IPv4 BGP4 routes in order to minimize the growth of the backbone IPv4 routing table. This active filtering of routes translates to a partial loss of inter-connectivity for the IPv4 Internet. Comparing the two routing systems shows the core IPv4 Internet routing systems has reached upwards of 130,000 routes while the IPv6 Internet has only about 350 routes. A comparison between the size and growth rates of the IPv4 and IPv6 BGP routing tables is shown in Figure 8.
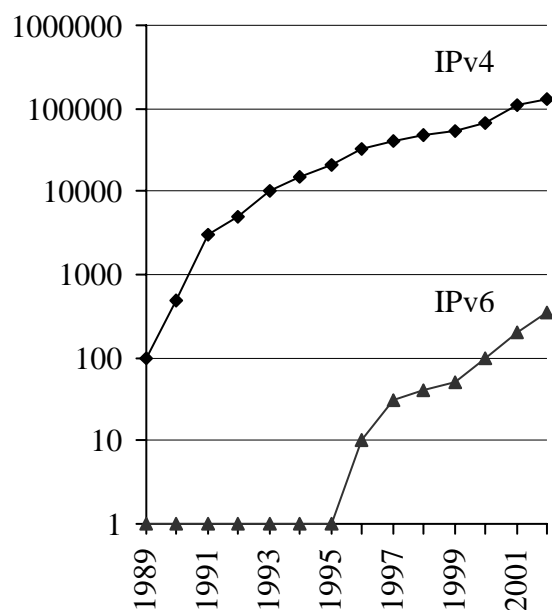
Figure 8. Comparison of IPv4 and IPv6 BGP Routing Tables

IPsec promises a new data privacy and authentication security service for the IPv6 Internet. All IPv6 compliant hardware and software products are required to fully support IPsec. It will be available, if desired, to secure all classes of traffic not simply TCP connections as common is today.

IPv6 will, in the mid to long-term, reduce the complexity, costs, and administration associated with USN and USMC

communications. Unfortunately, communications will likely become more complex, costly, and require additional administration during the short and mid-term while IPv4 is still dominant. The IPv6 protocol has been designed to automate network configuration to the greatest extent possible and therefore reduce operating costs.

c. New devices, applications, and services will be available with IPv6.

At least three critical applications have been identified which would require IPv6 for effective and ubiquitous use by the military. Voice Over IP (VOIP) is the first of these applications. VOIP can be deployed to a limited extent with IPv4 but cannot be utilized ubiquitously due to the deployment of NAT. IPv6 would be needed if VOIP was integrated into the NIPRNET to assume the functions of and eliminate the costs of the Defense Switched Network (DSN). IPv6's advanced Quality of Service (QoS) features also provide new capabilities to enable the integration of voice and video with data over the NIPRNET, SIPRNET, and JWICS.

Remote sensing is the second critical application requiring the use of IPv6 by the military. The integration of massive numbers of sensors into the DoD information grid could not be supported long by the current IPv4 protocol standard. Each remote sensor would likely require at least one unique IP address. The NIPRNET, SIPRNET, and JWICS routing systems would also need to grow to orders of magnitude greater capacity than today to support massive numbers of remote sensors.

Host mobility is the last critical application yet identified requiring the use of IPv6 by the military. The USN and USMC enterprise uses great numbers of mobile wireless computing devices for all sorts of tasks ranging from maintenance to security. IPv6 offers new capabilities to enable mobile wireless internetworking. Most of these new capabilities are not available with IPv4. The lack of available address space with IPv4 has also significantly hampered the deployment of mobile IP networking. The routing system must also scale to support these many new mobile wireless devices.

Many new products support both IPv6 and IPv4 in a dual stack capability. This is the most graceful co-existence means for hosts and end-system devices and also the most common offered by industry. Dual stacking does not necessarily mean these devices will have comparable capabilities with both protocols. Many devices will still need to utilize private IPv4 addresses and communications in the dual stacked model. These machines will only be able to have a domain name associated with their IPv6 address.

Certain products, such as 3G cellular phones, will soon be commercially available which are only capable of IPv6 communications. These products may not be unusable by the USN and USMC enterprise unless there is an existing IPv6 communications capability. The enterprise should consider this factor carefully since developing GOTS alternatives to COTS is expensive and problematic.

Microsoft recently announced a new capability for the Windows XP operating system called the Personal Area Network (PAN). PAN is supported only by the IPv6 protocol. It enables a group of devices to automatically form an ad-hoc network in a small area such as a desk or cubicle.

d. A new and growing Internet community is accessible via IPv6.

The USN and USMC enterprise must communicate with many organizations in order to accomplish it's mission. It has been demonstrated that many commercial, academic, and government organizations are adopting IPv6 as the new Internet protocol standard. These organizations have begun deploying IPv6 communications in parallel with their existing IPv4 communications. It is reasonable to assume that some of these organizations will retire their IPv4 communications quicker than others and quicker than the USN and USMC enterprise. The USN, USMC, and DoD should begin deploying IPv6 communications capabilities to ensure full interoperability with these organizations during both peace and wartime.

e. Enterprise self-synchronization could suffer during the transition from IPv4 to IPv6.

There are at least sixteen coexistence mechanisms for incorporating IPv6 into existing IPv4 communications. Some of these can be utilized stand alone, some can be used in combination, some must be utilized in combination, and some are intended for home use and not the enterprise.

The USN and USMC comprise many different programs and many different communities. During the transition period from IPv4 to IPv6, it is reasonable to believe that some programs and communities will embrace IPv6 faster than others. USN and USMC programs and communities are free to choose different sets of IPv6 co-existence mechanisms at any point in time without higher-level guidance. With this situation, interoperability between

systems and different communities may suffer for some period of time.

Administrators of existing IPv4 networks may be reluctant, at least initially, to embrace IPv6 just because it represents addition work and security threats. Others within those same organizations may begin work with IPv6 independent of existing administration. This can create an environment of animosity and competition verses cooperation and teamwork. Problems with applications and network services can arise when different administrators control IPv4 and IPv6 resources within an organization.

f. Expect increased operating costs, management complexity, and interoperability problems during the transition.

The resources required to effectively manage networks and systems utilizing both IPv4 and IPv6 will likely be greater than what is expended today with only IPv4. Infrastructure will be more difficult to configure and more complex to manage. Additional bandwidth may be required since IPv4 and IPv6 will likely operate over many of the same communications links. Operating costs could climb as existing resources are stretched and new resources marshaled to the task.

Interoperability may suffer during the transition since certain devices will be capable of communicating using one version of IP. IPv4 only devices will need to use translators to communicate with IPv6 only devices and vice versa. Translation is the least recommended coexistence mechanism since it has serious issues associated with it and may require significant Research and Development (R&D) to perfect.

g. There is concern for resources shared between the IPv4 and IPv6 Internets.

Many communication resources will likely be shared by the IPv4 and IPv6 protocols during the transition. This may lead to additional security vulnerabilities, contention for the resources, and inefficiencies. Care needs to be taken to managing these resources shared by the IPv4 and IPv6 protocols for the transition period however long it may be.

Both IPv4 and IPv6 share the forward DNS tree while the reverse DNS trees are separate. Interoperability will suffer if one administrator controls the forward DNS zone and the IPv4 reverse DNS zone while another administrator controls the IPv6 reverse DNS zone. This scenario may be very prevalent since most administrators of existing IPv4 networks are focused on "production" services. To experiment with IPv6, many Research and Development (R&D) activities may have to independently obtain IPv6 address space. The result of this is that a forward DNS query produces a consistent result for IPv4 and IPv6 while a reverse DNS query can produce two different results. Applications such as SMTP email may not work properly because they typically utilize the DNS for security.

Some router vendors have chosen to implement routing protocols, which share IPv4 and IPv6 configuration and processing. This may reduce the processing or memory requirements on routers running both protocols concurrently. It is unknown if a remote attack on an IPv6 routing protocol can impact the routing of a production IPv4 network but this is possible.

Tactical data links will have to carry IPv6 as well as IPv4 traffic sometime in the future if you believe there will be a transition. Bandwidth is a limited and precious quantity. Running IPv4 and IPv6 concurrently on a tactical data link could result in a reduction of useable bandwidth to the fleet. Additional bandwidth could mitigate this problem but would result in additional costs.

Memory in all sorts of devices will have to be shared when using IPv4 and IPv6. The memory in many routers is already taxed by the size of the IPv4 routing table. Adding IPv6 to these devices may result in memory overflows or may require the addition of memory if that is even possible.

h. Enterprise policies, processes, procedures, and databases will need modification to support IPv6.

Numerous policies, processes, and procedures in the USN and USMC enterprise assume the IPv4 protocol format and syntax. This is also the case in the wider DoD enterprise. These should be examined for impacts of incorporating IPv6. Potential modifications could span the spectrum from simple to extensive. New policies specific to IPv6 may also need to be issued. For example, see appendix A "Draft DoD Internet Protocol version 6 (IPv6) Guidance".

Information Assurance Vulnerability Alerts (IAVA) from the military Computer Emergency Response Team (CERT) currently assume the IPv4 protocol is the only Internet protocol. This is also the case for Naval Computer Incidence Response Team (NAVCIRT) advisories. For example, NAVCIRT advisory NA02-022 (appendix B) states "the following Internet Protocol (IP) addresses have recently been reported probing and/or attempting to access navy.mil computer systems. Recommend

system administrators block the following IP addresses at systems routers for a period to expire 30SEP2002". All the IP addresses in the advisory are dotted-decimal IPv4 addresses.

Many of the Military Network Information Center (MIL NIC) policies, processes, procedures, and databases currently assume IPv4 is the only Internet Protocol. It is understood MIL NIC management has begun scoping the effort required to incorporate IPv6 support. Details of MIL NIC IPv6 impacts have not yet been released. IPv6 as a minimum will impact the following MIL NIC functions:

- Management and allocation of IP addresses blocks.

- Management and administration of NIPRNET and SIPRNET DNS root servers.

- Management and assignment of domain names to IP addresses

- Management of forward DNS delegations.

- Management of reverse DNS delegations.

- Management of forward DNS zones.

- Management of reverse DNS zones.

- Management of IP address databases.

i. Network services need enhancements to support IPv6.

The USN and USMC enterprise will need to determine the best means of offering network services during the IPv4 to IPv6 transition period. There are a number of ways this can be accomplished effectively but operating costs will vary and information assurance will be impacted. An IPv6 transition strategy for the USN and USMC enterprise should address this in detail.

Each DNS forward and reverse zone is recommended to have at least two DNS servers, one primary server and one secondary server. The USN and USMC could dual stack each DNS server in the zone with IPv4 and IPv6 but risk the possibility of name service disruptions to both IPv4 and IPv6 communications with an IPv4 or IPv6 remote attack. This is likely the lowest cost solution but is the risk acceptable? As an alternative, the USN and USMC could maintain the two original IPv4 only DNS servers unchanged and procure two additional IPv6 only DNS servers. The forward and reverse zone files would then be manually replicated and maintained consistent. This is a higher cost alternative but more secure from remote attack.

DNS is the only network service that has been investigated through experimentation. Other network services such as network time and Public Key Infrastructure (PKI) should be similarly investigated. Each of these network services will likely have new vulnerabilities to IPv6 remote attack. It may also be impractical to separate the functions of some network services into IPv4 and IPv6 components if databases need to be maintained in real-time.

j. Enterprise COTS and GOTS infrastructure will need enhancements to support IPv6.

Many COTS infrastructure products shipping today have IPv6 capabilities already built in. Vendors have typically chosen not to "turn on" the IPv6 capabilities

of their products automatically out of the box. Administrators must manually configure IPv6, at this time, but this could change in the near future.

COTS infrastructure such as the Motorola Network Encryption System (NES) and GOTS infrastructure such as the Fastlane encryptor are understood to only support the IPv4 protocol standard. These COTS and GOTS products will require enhancements as IPv6 is deployed. In certain situations, Fastlane encryptors may be configured in ATM vs IP mode to alleviate this problem. In other situations, it may be more cost-effective to replace COTS and GOTS infrastructure devices than upgrade them to support both IPv4 and IPv6.

k. Enterprise COTS and GOTS applications will need enhancements to support IPv6.

Many COTS and open source software applications already have some level of IPv6 support built in. The maturity level of each of these is as of yet not well understood or independently documented. The development cycles for this class of software tend to be relatively rapid so new versions should be continually examined for IPv6 functionality and maturity.

Nearly all GOTS applications have no IPv6 capabilities at this time. Porting will not enable all the functionality and capabilities of IPv6 in GOTS applications just those that are already available with the current IPv4 software. Enabling advanced IPv6 features such as mobility, anycast addressing, and Quality of Service (QoS) will likely require additional software development, testing, and certification.

Porting applications to support both IPv4 and IPv6 may not require significant additional effort. Vendors have stated the effort was "more tedious than difficult". Developers can begin by downloading a scanning tool such as Sun's IPv6 Socket Scrubber or Microsoft's checkv4. These tools operate on source code to identify areas needing modification to support IPv6. Modifications can then be made to the source code and the software recompiled, tested, and certified for use. The Microsoft publication Adding IPv6 capability to an IPv4 Application divides the software porting effort into four areas. These areas are:

1. Changes to data structures.

2. Function call changes.

3. Removal of hard-coded IPv4 addresses.

4. Elimination of user interface issues.

It should be noted Microsoft has no plans to provide the IPv6 software libraries and function calls for the current USN and USMC enterprise operating system, Windows 2000. This complements Microsoft's strategy of providing a "production" IPv6 stack only for Windows XP and later versions of the Windows OS.

Some GOTS applications are actually conglomerations of COTS applications and some government developed code. Porting such an application might require a considerable coordination effort and involve multiple interdependencies. For example, how practical could porting a GOTS application be if a critical COTS software component was not yet ported to IPv6? In this case, a Program Manager (PM) might simply replace that software component with a different commercial alternative but then other code changes would likely be required.

l. IPv6 will impact new and ongoing enterprise acquisitions.

IPv6 support should be specified for all new acquisition programs as soon as possible. This will minimize future transition costs. Is this possible, at the same time, without an ASD-C3I or JTA mandate? Very few acquisition programs appear to be requiring IPv6 support today.

Support for IPv6 should be required today of COTS products. These products can be procured for operational systems without "turning on" or configuring the IPv6 capabilities. In essence, these products would be IPv4 only until some time in the future when the product's IPv6 capabilities are configured. This policy would minimize forklift upgrades when IPv6 is mandated.

GOTS software development programs should be required to use the new IPv6 software libraries, function calls, and APIs. These are now available in the newest commercial software development environments. The code can then be developed, tested, certified, and deployed in an IPv4 only operational environment. This GOTS software should then function with the IPv6 protocol with little modification when configured in the future.

m. IPv6 will significantly impact enterprise training.

Commercial industry has begun offering a few IPv6 training classes but no formal IPv6 training courses have been identified within the USN and USMC shore training establishment at this time. This may be due to a lack of awareness of the IPv6 issue. It could also be related to the fact IPv6 is still not a mandated standard but an emerging standard. This has resulted in a lack of operational experience with IPv6 communications throughout the USN and USMC enterprise. These are shortcomings, which should be addressed quickly since training classes take time to prepare and perfect. Training coursework should be in place before there is a major deployment of IPv6 to operational IP communications.

n. There is a need for an IPv6 Test and Evaluation (T&E) capability within the enterprise.

The USN and USMC enterprise should possess at least one T&E capability to assess all aspects of the IPv6 transition. In the long term, many will likely develop. SPAWAR Systems Center Charleston already leads one of these T&E capabilities called the DISN-LESv6. To date, T&E have focused on the fielding production dual stacked IPv4 and IPv6 communications. Future testing should include conformance testing, vendor interoperability testing, and product maturity testing.

The Draft DoD IPv6 Guidance (Appendix A) states "No implementations of IPv6 are permitted on networks carrying operations traffic within DoD at this time". The draft policy statement also states "DoD Components are encouraged to coordinate, undertake, and participate in IPv6 demonstrations/testbeds and share the results". While these two statements appear somewhat conflicting, they are actually not. DoD recognizes there is a clear need for an IPv6 T&E capability within the USN and USMC enterprise but it must be separate from operational DoD IPv4 communications to defend against remote IPv6 attacks. When USN, USMC, and DoD Information Assurance (IA) capabilities have ramped up to the challenges of defending against IPv6 remote attack, IPv6 can be enabled on operational networks for T&E purposes. Until that date, costs will be

greater to perform IPv6 T&E functions within the USN and USMC enterprise.

o. Enterprise IA capabilities will need to be enhanced to support IPv6.

Any device understanding the IPv6 protocol and somehow connected to the IPv6 Internet is vulnerable to remote attack via IPv6. Many of the vulnerabilities associated with IPv4 communications will also be present with IPv6 communications. New vulnerabilities exist with IPv6 due to new features and IPv6 coexistence mechanisms. Few COTS firewall products have been found which support the IPv6 protocol. Firewall vendors may be slower to integrate support for IPv6 than other sectors of industry. This could be due to a potential architectural conflict between E2E IPsec and firewalls. Firewalls typically expect to see packet headers in plaintext. They allow certain packets through based on the packet headers and others are discarded. To date, only one commercial firewall vendor has publicly announced support for IPv6. At least three open source software firewall products claim to support the IPv6 protocol. The maturity and capabilities of these firewalls have not yet been tested and is not well understood.

No COTS Intrusion Detection Systems (IDSs) have been found that support the IPv6 protocol. One open source IDS has been found but this software is highly suspect. A potential architectural conflict exists between IDSs and E2E IPsec similar to that with firewalls. IDSs are critical to the protection and operation of our unclassified IP networks. The USN and USMC may require the development of a GOTS IPv6 IDS if at least one commercial source is not identified in the near future.

p. Enterprise Offensive Information Warfare (IW) capabilities will need to be enhanced to support IPv6.

Electronic intelligence collection is a component of the USN and USMC information warfare mission. The IPv6 Internet already has a broad spectrum of users. Most of these are likely friendly or neutral to the USN and USMC enterprise but some will likely not be. It is assumed the IPv6 Internet has or will have shortly a community of hackers, crackers, criminals, and potential adversaries just like the IPv4 Internet. For example, articles in the press have stated that Al Qaeda operatives are using the IPv4 Internet to communicate with their leadership and coordinate attacks on the US. It is also possible they may be using the IPv6 Internet for a similar purpose. The USN and USMC enterprise should be able to intercept and collect intelligence from IPv6 Internet communications as a component of its information warfare capabilities. It should be able to do so as it already possesses this capability for IPv4 Internet communications.

Disruption of enemy communications is also a component of the USN and USMC information warfare mission. It is unknown how many enemies of the US may already be utilizing IPv6 communications or how mature their communications are. The USN and USMC enterprise should be able to disrupt IPv6 communications as a component of its information warfare capabilities. It should be able to do so as it already possesses this capability for IPv4 Internet communications.

q. IPv6 may significantly impact the financial condition and available resources of the enterprise.

To date, very modest resources have been applied to experimentation with IPv6. Resources have not been adequate to perform comprehensive and in-depth studies and experimentation. If and when IPv6 is mandated as a standard by ASD-C3I and/or the JTA, these resources will need to be quickly expanded. Resources will be needed to train engineers and support personnel. An IPv6 T&E capability will need to expand to reach all necessary USN and USMC organizations. Testing will need to be expanded to include conformance testing, vendor interoperability testing, and product maturity testing. Additional hardware and software may well be needed depending on how IPv6 is deployed. If deployed on existing infrastructure, hardware and software costs could be minimal but securing this infrastructure will be more difficult. If deployed on separate and distinct infrastructure, costs will be higher but IA may be simplified. This all translates to the need for additional funding and resources.

Many existing contracts, such as the Navy and Marine Corp Intranet (NMCI) may need to be adjusted or renegotiated if IPv6 is mandated. Additional effort will be required for prime contractors and subcontractors to build and maintain and IPv6 capability in systems currently under contract but not specifically specifying IPv6. These additional costs are not well understood at this time.

USN and USMC enterprise Program Objective Memorandums (POMs) will need to be adjusted to include adequate resources for comprehensive IPv6 studies, experimentation, and deployment. They should also be adjusted to include funds for the eventual retirement of IPv4 in the distant future.

8. Conclusions and Recommendations

The USN and USMC enterprise should develop a comprehensive IPv6 transition strategy to maximize the benefits and minimize the negative impacts and costs to the fleet. While the timing and speed of a commercial move to IPv6 is not at all clear at this time, much of the world is already on the path of transition. Although not ubiquitous yet, many IPv6 capable products exist today. It is unclear how long IPv4 products will be ubiquitous or commercially available.

It is doubtful the IPv4 protocol can realize the concept of FORCENET being an information grid reaching from seabed to outer space. The IPv4 protocol is already nearing the limits of its capabilities. FORCENET will require orders of magnitude more devices integrated into the information grid. Each of these devices will require at least one IP address and the full peer-to-peer capabilities of IP. Effective and ubiquitous deployment of VOIP, remote sensing, and host mobility within FORCENET and the USN and USMC enterprise will require the use of the IPv6 protocol.

The Expeditionary Command, Control, Communications, Computers, Combat Systems Grid (EC5G) program should consider leveraging the existing IPv6 knowledge, expertise, and capabilities of the USN and USMC to realize the vision of FORCENET. SPAWAR Systems Center Charleston (SSCC) already possesses a comprehensive IPv6 experimentation capability. Nearly all the information in this report was collected from the

experimentation at SSCC over the DISN-LESv6 pilot network. Many additional forms of T&E will be needed in the future to properly manage the transition to IPv6.

POMs should soon be adjusted to incorporate resources for the safe and effective incorporation of IPv6 into USN and USMC communications. In the distance future, USN and USMC POMs will need to incorporate resources for the retirement of the current IPv4 standard. These POM adjustments should be accomplished in close coordination with the remainder of the DoD community.

IPv6 compliance in new and existing acquisition programs should be encouraged to minimize transition costs. Commercial products can be procured today with both IPv4 and IPv6 capabilities. IPv6 capabilities of COTS products do not initially need to be enabled.

USN and USMC enterprise IA and IW capabilities will need enhancements to include support for the IPv6 protocol. There is already a large global IPv6 Internet and a growing international community of IPv6 users. This community likely contains hackers, crackers, criminals, and potential adversaries just like the IPv4 Internet. It will be necessary to protect USN and USMC communications from remote IPv6 attack. It should also be important to collect intelligence from and disrupt the IPv6 communications of adversaries.

New GOTS application software should be developed to support the IPv6 protocol. Application software can be developed which is "agnostic" to the IP version in use. This will minimize transition costs but may require the adoption of "next generation" COTS OSs in place of the current generation USN and USMC enterprise

operating systems such as Windows 2000. Many "next generation" COTS operating systems are already commercially available. These will likely include a number of IPv6 ported applications. They should also contain production IPv6 stack software, IPv6 software libraries, and IPv6 development tools that are needed for effective GOTS application porting.

Training should be developed and provided to educate the USN and USMC enterprise work force with respect to all aspects of the IPv6 transition. Without effective training, transition costs will likely be higher and negative impacts compounded. Readiness could also suffer if the fleet is utilized as the classroom for IPv6 training instead of the USN and USMC shore training establishment.

APPENDIX A

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
      CHAIRMAN OF THE JOINT CHIEFS OF STAFF
      UNDER SECRETARIES OF DEFENSE
      DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
      ASSISTANT SECRETARIES OF DEFENSE
      GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
      INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
      DIRECTOR, OPERATIONAL TEST AND EVALUATION
      ASSISTANTS TO THE SECRETARY OF DEFENSE
      DIRECTOR, ADMINISTRATION AND MANAGEMENT
      DIRECTORS OF THE DEFENSE AGENCIES
      DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Internet Protocol Version 6 (IPv6) Guidance

    This memorandum provides initial DoD guidance for fielding IPv6. Currently, Internet Protocol Version 4 (IPv4) represents the fundamental mandated internetworking protocol for the DoD. It is essential that such a fundamental change to our Internet Protocol (IP)-based information systems be well planned and only undertaken once there is a thorough understanding of involved costs and impacts on Global Information Grid (GIG) system performance, interoperability, and security.

    IPv6 is the next generation network layer protocol of the Internet as well as the GIG including NIPRNET, SIPRNET, JWICs, and most emerging DoD space and tactical communications. IPv6 is becoming necessary due to fundamental limitations in the current IPv4 protocol that makes IPv4 incapable of meeting long-term requirements of the commercial community. IPv6 is designed to overcome those limitations by expanding available IP address space to accommodate the worldwide explosion in Internet usage, improving end-to-end security, facilitating mobile communications, providing new enhancements to quality of service, and easing system management burdens. Furthermore, IPv6 is designed to run well on the most current high performance networks (e.g. Gigabit Ethernet, OC-12, ATM, etc.) and without experiencing a significant decrease in capacity on low bandwidth systems.

    While the timing and speed of a commercial move to IPv6 is uncertain, it is expected to gradually replace IPv4 over the next several years. The tremendous capital investments in IPv4 technology by users worldwide will likely result in an extended transition period where both protocols coexist. An upgrade to IPv6 presents DoD with a number of major challenges that must be addressed through an overall enterprise strategy. That strategy has to consider operational requirements, information assurance, and costs while maintaining interoperability within the Department, across the Federal Government, among our allies, and with coalition partners in addition to the civilian and commercial sectors. This overall strategy will be part of the integrated GIG architecture, in harmony with any Federal level initiatives and in

concert with industry and international standards-making bodies. This memo provides the initial guidance to ensure that a DoD strategy is in-place and maintained.

It is DoD policy for all Information Technology (IT), communication and National Security Systems (NSS) which make up the GIG, that:

No implementations of IPv6 are permitted on networks carrying operations traffic within DoD at this time. This is consistent with the latest Joint Technical Architecture (JTA), which cites IPv4 as a "mandated standard" for IP-based solutions and the initial results of the information assurance risk assessment of IPv6 security implications, done by the Information Assurance Panel of the Military Communications Electronics Board. These implementation guidelines will be reconsidered once the Information Assurance risk assessment indicates that sufficient protection products are available and the IPv6 implementation plan (below) is completed and reviewed by the DoD CIO.

DoD Components and Services are encouraged to coordinate, undertake, and participate in IPv6 demonstrations/testbeds and share the results. This will ensure that DoD has the thorough understanding of the operational, security, interoperability and cost impacts needed to engineer a smooth transition to IPv6, at the appropriate time. However such demonstrations/testbeds of IPv6 should be reported to the DISA to ensure efforts are coordinated and integrated into DoD implementation planning (see below). Moreover, to minimize the risk to DoD at this time (see first paragraph in this section) those demonstrations/testbeds which leave local enclaves should use networks that do not carry operations traffic such as the Defense Research and Engineering Network (DREN), DISN Leading Edge Service (LES) or commercial services. A GIG network waiver is not required for demonstrations/testbeds to use these services. Applicable certification & accreditation processes must be followed for all implementations.

DoD activities acquiring new or upgrading existing IP-based technologies or services must recognize IPv6 readiness/compatibility as a likely future need. This is consistent with IPv6 being identified as an "emerging standard" in the JTA. As with other standards, the JTA configuration management process is the mechanism for considering any changes to mandated/emerging standards.

Defense Information Systems Agency (DISA) is directed to acquire IPv6 address space sufficient to meet DoD's five year requirements, and initiate acquisition of IPv6 address to meet **all** future DoD requirements by 30 Dec 02.

DISA will continue to manage DoD IP address allocation, registration and control on an enterprise basis to promote interoperability and security. This reaffirms a January 22, 1998 memorandum designating DISA as the DoD Central Registration Authority (CRA) for assignment and registration of Internet Protocol (IP) address space for any and all DoD sponsored data networks and systems. DISA will establish and maintain

an effective program for accurate management and accounting of all DoD-owned IP addresses.

DoD users will only acquire IP address space originating from DISA.

Finally, DISA is tasked to lead (in coordination with the DoD Chief Information Officer (CIO), and the Joint Staff with the support of DoD Components and Services) the effort to develop an initial implementation plan within six months from the date of this memo. The IPv6 implementation plan for DoD will address areas such as:

- Recommended technical migration strategy which recognizes coexistence requirements, protects interoperability, enhances security, and includes criteria for migration for fixed and tactical platforms (these recommendations should also be input and coordinated with GIG Architecture Version 2.0).

- Identification of what needs to be done to ensure readiness for migration, resources required to accomplish the migration, and organizational roles and responsibilities. This should include the addressing of IPv6 within the JTA.

- Identification of additional policy guidance needed.

The ASD (C3I)/DoD CIO focal point for this effort is Ms. Marilyn Kraus, who can be reached at (703) 607-0255 or marilyn.kraus@osd.mil.

Mr. Stenbit signature

APPENDIX B

ADMINISTRATIVE MESSAGE

ROUTINE

R 261301Z AUG 02 ZYB PSN 813600J18

FM FLTINFOWARCEN NORFOLK VA//N3//

TO ALCND

INFO CNO WASHINGTON DC//N6/N614/N6143/N2/N312/N515//
CNO WASHINGTON DC//N6/N614/N6143/N2/N312/N515//
CMC WASHINGTON DC//P/C4I/PLI/CSB/CIS//
CMC WASHINGTON DC//P/C4I/PLI/CSB/CIS//
USCINCSPACE PETERSON AFB CO//J3/J39/J6//
USCINCJFCOM NORFOLK VA//J3/J6//
USCINCJFCOM NORFOLK VA//J3/J6//
CINCLANTFLT NORFOLK VA//N6/N02C/N3/5/7-IW//
CINCPACFLT PEARL HARBOR HI//N3DC/N6/N69//
CINCPACFLT PEARL HARBOR HI//N3DC/N6/N69//
CINCUSNAVEUR LONDON UK//N3/N6/N9//
CINCUSNAVEUR LONDON UK//N3/N6/N9//
COMNAVNETWARCOM NORFOLK VA//N3/N6/N9//
COMNAVNETWARCOM NORFOLK VA//N3/N6/N9//
COMUSNAVCENT//N3/N39/N6//
COMUSNAVCENT//N3/N39/N6//
JTF-CNO WASHINGTON DC//J3/J6/LECIC//
NCTF-CND WASHINGTON DC//N3/N5//
NAVNETSPAOPSCOM DET WASHINGTON DC//N3/N65//
DIRNAVCRIMINVSERV WASHINGTON DC//20/22//
NAVNETSPAOPSCOM GNOC DET NORFOLK VA//N2/N3//
NMCI RNOC NORFOLK VA//N2/N3//
NMCI RNOC SAN DIEGO CA//N2/N3//
MITNOC QUANTICO VA//JJJ//
MITNOC QUANTICO VA//JJJ//
AFIWC LACKLAND AFB TX//EAA//
ACERT FT BELVOIR VA//JJJ//
NRO WASHINGTON DC//COM-EMOC/OSF//
DISA WASHINGTON DC//ASSIST//
DISA WASHINGTON DC//ASSIST//
HQ NORAD COMMAND CTR CHEYENNE MOUNTAIN AFS CO//CC/ND/
    J3/J39//
CMOC CHEYENNE MOUNTAIN AFS CO//NBMC//

CMOC CHEYENNE MOUNTAIN AFS CO//NBMC//

THIS IS A 4 SECTIONED MSG COLLATED BY MDS
UNCLAS //N05239//
PASS TO LAN ADMINISTRATOR, ISSM,
OR TECHNICAL HELP DESK
ALCND 044/02

MSGID/GENADMIN/FLTINFOWARCEN//

SUBJ/NAVCIRT ADVISORY 02-22 - RECOMMENDED IP BLOCK LIST
/PART ONE OF TWO - PART TWO IDENT 261302Z AUG 02//

REF/A/RMG/FLTINFOWARCEN/251301ZJUL2002//

REF/B/RMG/FLTINFOWARCEN/251302ZJUL2002//

REF/C/DOC/CNO/03MAR1998//

NARR/REFS A AND B ARE PARTS ONE AND TWO OF NAVCIRT
ADVISORY 02-20 RECOMMENDED IP BLOCKAGE. REF C IS OPNAVINST
2201.2 WHICH OUTLINES DON POLICY FOR COMPUTER INCIDENT
REPORTING.//
POC/MARI KIRBY/CIV/FLTINFOWARCEN/-/TEL: (757) 417-4187/
(DSN) 537-4187//

RMKS/1. THIS MESSAGE CANCELS REF A AND B.

2. THE FOLLOWING INTERNET PROTOCOL (IP) ADDRESSES HAVE
RECENTLY BEEN REPORTED PROBING AND/OR ATTEMPTING TO ACCESS
NAVY.MIL COMPUTER SYSTEMS. RECOMMEND SYSTEM ADMINISTRATORS
BLOCK THE FOLLOWING IP ADDRESSES AT SYSTEM ROUTERS FOR A
PERIOD TO EXPIRE 30 SEP 2002. THIS RECOMMENDATION DOES NOT
SUPERCEDE USE OF ONE OF THESE SPECIFIC IP ADDRESSES IF
REQUIRED FOR MISSION ACCOMPLISHMENT.
12.100.127.50, AT&T, US, SSH ACCESS
12.101.60.3, AT&T, US, HTTP ACCESS
12.150.192.40, AT&T, US, ATTEMPTED DOS
12.151.162.61, ARAMCO SERVICES CO, US, FTP ACCESS
12.224.141.24, AT&T, US, RCERT BLOCK
12.224.34.6, AT&T, US, RCERT BLOCK
12.24.129.170, MERCEDES HOMES, INC., US, HTTP ACCESS
12.252.50.60, AT&T, US, RCERT BLOCK
12.43.230.64, AQUARIUS ENT, US, SSH
12.46.138.139, XENOGEN CORP, US, SSH
128.101.220.28, ISLES.SPA.UMN.EDU, US, TELNET ROOT ACCESS

128.103.101.114, HARVARD UNIVERSITY, US, SSH SCAN
128.121.2.141, VERIO DATA CENTER, US, HTTP ACCESS
128.138.175.118, UNIVERSITY OF COLORADO, US, MULTIPLE ROOT ACCESSES
128.148.208.131, BROWN UNIVERSITY, US, PORT 1025
128.151.63.128, UNIVERSITY OF ROCHESTER, US, SSH SCAN
128.163.209.105, UNIVERSITY OF KENTUCKY, US, SSH SCAN
128.169.32.181, UNIVERSITY OF TENNESSEE, US, REMOTELY ANYWHERE
128.173.201.129, VSPA.VPSA.VT.EDU, US, HTTP ACCESS
128.208.44.201, D-128-208-44-201.DHCP.WASHINGTON.EDU, US, PORT 1025
128.208.67.29, UNIVERSITY OF WASHINGTON, US, SSH
128.242.252.129, WWW.SPEEDBIT.COM, IL, ADWARE
128.248.82.44, UNIV OF ILLINOIS, US, RCERT BLOCK
128.253.161.132, CORNELL UNIVERSITY, US, PORT 1025
128.39.12.100, NTANET, NO, SSH
128.46.125.117, ESEIPC-1.ECN.PERDUE.EDU, US, PORT 1025
128.59.141.35, COLUMBIA UNIVERSITY, US, TELNET ROOT ACCESS
128.61.32.232, ES.GATECH.EDU, US, PORT 1025
128.86.8.123, NTP0.JA.NET, GB, UNKNOWN
129.171.219.23, UNIV OF MIAMI, US, RCERT BLOCK
129.171.93.220, ADMIN1.MED.MIAMI.EDU, US, UNKNOWN
129.41.2.169, IBM CORP, US, SSH
129.49.109.230, DHCP-230-109.AMS.SUNYSB.EDU, US, PORT 1025
129.7.91.218, PC23514.DHCP.UH.EDU, US, PORT 1025
129.71.49.58, WEST VIRGINIA NETWORK FOR EDUC, US, PORT 1025
129.79.94.96, IU-MATH-96.MATH.INDIANA.EDU, US, ROOT ACCESS
130.149.134.79, TECHNISCHE UNIVERSITAET, DE, SSH
130.228.106.60, UNI2 INTERNET, DK, SSH
130.85.179.84, UNIVERSITY OF MARYLAND, US, SSH
130.91.152.229, UNIVERSITY OF PA, US, FTP ACCESS
131.152.102.64, UNIVERSITY OF BASEL, CH, SSH
131.159.24.7, INSTITUT FUER INFORMATIK, DE, SSH
132.254.215.22, SCORPION.GDA.ITESM.MX, MX, HTTP ACCESS
133.24.40.X, YAMAGATA UNIVERSITY, JP, HTTP ACCESS
133.38.1.X, SAITAMA UNIVERSITY, JP, HTTP ACCESS
134.100.2.X, UNIVERSITY OF HAMBURG, DE, SSH
134.210.115.112, STOCKTON STATE COLLEGE, US, SSH 1.0
134.28.77.54, TU-HAMBURG-GARBURG, DE, FTP ACCESS
134.96.172.140, UNIVERSITY OF THE SAARLAND, DE, SSH
138.110.7.230, MOUNT HOLYOKE COLLEGE, US, NIMDA
138.23.159.120, UNIVERSITY OF CALIFORNIA, US, NIMDA
138.4.10.161, TECHNICAL UNIVERSITY OF MADRID, ES, NIMDA
138.49.132.235, UNIVERSITY OF WISCONSIN, US, NIMDA
140.239.231.216, HARVARDNET, US, RCERT BLOCK
141.223.86.151, POHANG INSTITUTE OF SCIENCE, KR, HTTP ACCESS
142.166.92.37, IP142166092037.NBTEL.NET, CA, DENIAL OF SERVICE
142.176.134.28, STENTOR NATIONAL INTEGRATED CO, CA, MSTREAM

142.214.155.5, HUMBER COLLEGE, CA, HTTP ACCESS
142.227.29.2, CANADIAN DEPT OF EDUCATION, CA, RCERT BLOCK
143.169.159.4, UNIVERSITY OF ANTWERP, BE, FTP ACCESS
143.248.139.221, IDOS.KAIST.AC.KR, KR, ACCESS
144.13.204.23, UNIVERSITY OF WISCONSIN, US, HTTP ACCESS
144.136.0.202, TELESTRA, AU, HTTP ACCESS
144.136.102.95, TELESTRA, AU, HTTP ACCESS
144.136.236.134, TELESTRA, AU, RCERT BLOCK
144.214.5.107, CITY POLYTECHNIC OF HONG KONG, HK, HTTP ACCESS
144.230.240.2, SPRINT, US, HTTP ACCESS
146.201.30.58, FLORIDA STATE UNIVERSITY, US, SSH
147.162.53.84, UNIVERSITA PADOVA, IT, RCERT BLOCK
147.208.175.70, WWW.ONFLOW.COM, US, ADWARE
148.244.65.12, PEMSTAR DE MEXICO, MX, RCERT BLOCK
148.63.106.192, SPACENET INC., US, RCERT BLOCK
150.19.16.X, HIROSHIMA INST. OF TECHNOLOGY, JP, HTTP ACCESS
150.217.19.110, TELEMACO.DE.UNIFI.IT, IT, MSTREAM
150.49.132.82, CTINET, JP, HTTP ACCESS
151.199.156.233, BELL ATLANTIC, US, FTP ROOT ACCESS
151.200.243.215, BELL ATLANTIC, US, RCERT BLOCK
152.101.106.155, HK INTERNET, HK, RCERT BLOCK
152.31.128.165, NC RESEARCH NETWORK, US, SSH
152.63.100.X, UUNET, US, RCERT BLOCK
152.63.49.X, UUNET, US, RCERT BLOCK
152.63.85.X, UUNET, US, RCERT BLOCK
155.210.157.148, UNIVERSIDAD DE ZARAGOZA, ES, HTTP ACCESS
155.210.88.146, UNIVERSIDAD DE ZARAGOZA, ES, MSTREAM
155.58.118.41, LOUISIANA STATE UNIVERSITY MED, US, DENIAL OF SERVICE
159.43.254.100, EJV PARTNERS, US, SSH
159.62.86.160, THE TITAN CORP, US, FTP ACCESS
160.81.65.33, SPRINT, US, SMTP ATTEMPTED DOS
161.111.222.4, CSICNET, ES, HTTP ACCESS
161.142.183.172, MIMOS, MY, HTTP ACCESS
161.58.9.10, VERIO, INC., US, FTP ACCESS
163.180.105.92, KYUNGHEE UNIVERSITY, KR, RCERT BLOCK
165.234.63.124, IS DEPT STATE OF N. DAKOTA, US, SSH
167.216.132.211, S20000052SU05.FPLIVE.NET, US, PORT 6970 GATE CRASHER
168.160.156.130, STATE SCIENCE & TECHNOLOGY, CN, HTTP ACCESS
168.229.1.50, BERGEN COUNTY SCHOOL DISTRICT, US, MALICIOUS ACTIVITY
172.180.96.232, AOL, US, HTTP ACCESS
172.183.99.248, ACB763F8.IPT.AOL.COM, US, ROOT ACCESS
PASS TO LAN ADMINISTRATOR, ISSM,
OR TECHNICAL HELP DESK
ALCND 044/02

MSGID/GENADMIN/FLTINFOWARCEN//

SUBJ/NAVCIRT ADVISORY 02-22 - RECOMMENDED IP BLOCK LIST
172.184.243.244, AOL, US, FTP ACCESS
172.190.11.66, ACBEOB42.IPT.AOL.COM, US, RCERT BLOCK
192.228.128.20, MALAYSIAN INSTITUTE OF MICROEL, MY, HTTP ACCESS
192.244.23.1, IRC.TOKYO.WIDE.AD.JP, JP, DENIAL OF SERVICE
192.6.173.11, HEWLETT PACKARD, US, RCERT BLOCK
193.104.202.66, ISLANDIS.NET, FR, SSH
193.11.232.123, CHALMERS-GU-STUDENT, SE, FTP ACCESS
193.11.251.5, CHALMERS-GU-STUDENT, SE, MS SQL ACCESS
193.113.53.133, BT CORPORATE, GB, FTP ACCESS
193.141.169.186, XLINK-TRANSIT-ISAR, DE, SSH
193.15.196.125, BYGGSTANDARDISERINGEN, SE, HTTP ACCESS
193.231.207.117, DNT TIMISOARA, RO, HTTP ACCESS
193.232.91.229, ROSPRINT COMPANY, RO, DENIAL OF SERVICE
193.253.181.115, FRANCE TELECOM, FR, IDS MAPPING
193.38.143.9, THURROCK COLLEGE, GB, SSH
193.45.189.163, MELTINGPOINT.COM, US, ADWARE
193.5.0.70, CUBENET, CH, SSH
194.153.243.168, REGAL-NET, RO, ACCESS
194.168.80.251, DIAMOND CABLE COMMUNICATIONS, GB, ROOT ACCESS
194.19.28.135, NO-WWW-NORGE, NO, SSH
194.202.188.51, IMAGIC UK PLC, GB, DENIAL OF SERVICE
194.219.104.173, FOTHNET, GR, HTTP ACCESS
194.225.70.80, INSTITUTE FOR STUDIES, IR, FTP ROOT ACCESS
194.226.201.199, DIZLA NETWORKS, RU, SOCKS PORT 1080
194.236.142.178, AS3-6-.KA.G.BONET.SE, SE, BOTNET
194.244.83.5, UNICSOURCE.IT, IT, FTP
194.65.120.34, PORTUCEL, PT, FRAGMENTED PACKETS
194.65.139.100, PORTUCEL, PT, FRAGMENTED PACKETS
194.65.35.221, PORTUCEL, PT, FRAGMENTED PACKETS
194.65.64.12, PORTUCEL, PT, FRAGMENTED PACKETS
194.72.6.103, BRITISH TELECOMMUNICATIONS, UK, DNS ACCESS
194.73.73.113, BRITISH TELECOMMUNICATIONS, GB, ROOT ACCESS
194.78.32.252, CYBER CLUB INTERNET, BE, SSH
194.85.32.X, NS.RUNNET.RU, RU, RING ZERO
195.101.51.38, GOV.SYSTRANSOFT.COM, FR, SOCIAL ENGINEERING
195.14.253.217, NETCOLOGNE GMBH, DE, SSH
195.146.32.248, TELECOMUNICATION OF IR, IR, HTTP ACCESS
195.146.51.101, EMAMREZA-NET, IR
195.151.104.X, KRASNODAR CELLULAR, RU, HTTP ACCESS
195.158.245.X, EBONE VIENNA, AT, RCERT BLOCK
195.162.210.204, TVD-INTERNET, IT, ACCESS
195.182.163.27, DIAMOND CABLE COMMUNICATIONS, GB, PORT 2000 ROOT
ACCESS
195.2.0.89, CABLE & WIRELESS, AT, HTTP ACCESS

195.2.124.82, DELFI-ETH, LV, SSH
195.205.160.74, ZRIT-OLSZTYN, PL, MSTREAM
195.226.127.98, GESELSCHAFT FUER NETZWERKMANAGEMENT, DE, SSH
195.232.54.13, FRANKFURT PPP CLIENT POOL, DE, RCERT BLOCK
195.247.33.99, SHD DATENTECHNIK, DE, SSH
195.54.193.202, RINET ISP PROJECT, RU, DENIAL OF SERVICE
195.6.173.240, AFPA, FR, FTP ACCESS
195.70.180.10, WMDATA INTRATEC/CIMTEC, NO, HTTP ACCESS
195.74.0.20, SCIFI, FI, ACCESS
195.80.171.154, PSG-SK, SK, RCERT BLOCK
195.94.213.176, POLISH REGIONAL TELECOMMUNICATION, PL, RCERT BLOCK
196.40.2.34, EMBAJADA, CR, RCERT BLOCK
196.40.3.62, AMNET TELEVISION, CR, HTTP ACCESS
198.142.1.243, OPTUS COMMUNICATIONS, AU, BOTNET
198.180.59.30, BUSINESS INTERNET, US, HTTP ACCESS
198.22.51.115, LOGINE.V, DE, RCERT BLOCK
198.30.116.7, OARNET, US, SSH
198.59.2.114, AURARIA HIGH EDUCATION, US, HTTP ACCESS
199.174.197.164, S2F ONLINE, US, SSH
199.175.103.17, NORTHERN COMPUTER PRODUCTS, US, SSH
199.182.243.148, ICG NETAHEAD, INC., US, HTTP ACCESS
199.232.158.222, CAMBRIDGE ENTREPRENEURIAL, US, SSH
199.232.158.58, WWW.MESSAGEMATES.COM, GB, ADWARE
199.45.65.136, COMBATSIM.COM, CA, HTTP ACCESS
199.72.71.121, ACCUCOPY OF GREENVILLE, US, HTTP ACCESS
200.164.0.X, COMITE GESTOR DA INTERNET NO BRASIL, BR, SSH
200.168.78.X, COMITE GESTOR DA INTERNET, BR, HTTP ACCESS
200.177.97.X, COMITE GESTOR DA INTERNET NO BRASIL, BR, SSH
200.184.194.X, INTELIG TELECOMUNICACOES LTDA., BR, PORT 2000 ROOT
ACCESS
200.189.56.X, NET21 CONECTIVADADE LTDA, BR, HTTP ACCESS
200.193.92.X, INTERNET GROUP DO BRASIL, BR, HTTP ACCESS
200.195.52.X, CENTRO DE GENENCIA DE REDE, BR, HTTP ACCESS
200.203.236.X, COMITE GESTOR DA INTERNET, BR, HTTP ACCESS
200.214.38.X, COMITE GESTOR DA INTERNET NO BRASIL, BR, SSH
200.224.139.X, GLOBAL ONE, BR, TELNET ACCESS
200.226.110.X, INTERNET GROUP DO BRASIL, BR, HTTP ACCESS
200.248.162.X, BATANOLI, BATANOILI E SOUZA LTD, BR, FTP ROOT ACCESS
200.254.62.X, COMITE GESTOR DA INTERNET NO BRASIL, BR, SSH
200.28.86.67, COMPANIA MINERA VALDIVAR, CL, RCERT BLOCK
200.43.177.81, ALICIA MOREAU DE JUSTO, AR, SSH
200.53.234.124, UNIVERSIDAD AUTONOMA BENITO JUAREX DE OAXACA, MX,
HTTP ACCESS
202.1.192.211, DHIVEHI RAAJJEYGE GULHUN, MV, HTTP ACCESS
202.102.133.39, SHANDONG TELECOM, CN, HTTP ACCESS
202.102.180.23, CHINANET, CN, RCERT BLOCK

202.102.224.X, HENAN MULTIMEDIA, CN, NMAP
202.103.209.X, CHINANET, CN, ROOT ACCESS
202.105.36.X, CHINANET GUANGDONG PROVINCE, CN, HTTP ACCESS
202.106.208.X, CHINANET BEIJING PROVINCE, CN, HTTP ACCESS
202.108.33.X, CHINA TELECOM, CN, HTTP ACCESS
202.109.73.X, SHANGHAI ONLINE, CN, MISC PORT SCANS
202.111.83.X, CHINANET, CN, HTTP ROOT ACCESS
202.111.88.X, CHINA TELECOM, CN, WEB HACK
202.118.68.X, DALIAN UNIVERSITY, CN, HTTP ACCESS
202.130.147.X, UUNET TECHNOLOGIES, HK, WEB TRAVERSAL
202.149.82.X, SATNET, ID, FTP ACCESS
202.155.35.X, TRIAL YOGYAKARTA, ID, HTTP ACCESS
202.161.134.X, ORION, TW, HTTP EXPLOITS
202.179.0.81, MICOM CO, MN, SSH
202.181.246.X, HONGKONG COMMERCIAL, HK, FTP
202.202.216.X, CQERNET, CN, HTTP ACCESS
202.204.113.X, BEIJING FORESTRY UNIVERSITY, CN, HTTP ACCESS
202.227.192.X, HIGH SPEED INFO, JP, SSH
202.29.18.X, UNINET, TH, SSH
202.4.254.X, SPARKICE, CN, INTERNET CAFI
202.54.37.X, VSNL, IN, HTTP ACCESS
202.67.145.X, HKNET, HK, HTTP ACCESS
202.79.79.X, EMECCA CONSULTING, SG, MS SQL ROOT ACCESS
202.85.176.X, CHINA COMPUTER CONSULTANTS, CN, ACCESS
202.90.77.X, NETSOL TECHNOLOGIES, TW, HTTP ACCESS
202.96.0.X, CHINANET, CN, SMTP ATTEMPTED DOS
PASS TO LAN ADMINISTRATOR, ISSM,
OR TECHNICAL HELP DESK
ALCND 044/02

MSGID/GENADMIN/FLTINFOWARCEN//

SUBJ/NAVCIRT ADVISORY 02-22 - RECOMMENDED IP BLOCK LIST
202.97.215.X, DATA COMMUNICATIONS, CN, HTTP ACCESS
202.97.224.X, CHINANET, CN, ACCESS
202.99.176.X, CHINANET, CN, HTTP ACCESS
203.117.136.X, HORIZONTECH, SG, ACCESS
203.122.0.X, SPECTRANET, IN, RCERT BLOCK
203.126.18.238, MONA COMPUTER SYSTEMS, SG, RCERT BLOCK
203.126.46.98, INTERNATIONAL SQL STAR, SG, MS SQL
203.130.8.116, SUPER8-LINE-116.SUPER.NET.PK, PK, JOAN
203.134.5.9, PRIMUS, AU, RCERT BLOCK
203.140.38.X, NICHIZEI INTERNET, JP, HTTP ACCESS
203.146.74.X, MINISTRY OF EDUCATION, TW, RCERT BLOCK
203.149.149.X, EASTNET, TW, FTP
203.169.186.X, HKNET, HK, DENIAL OF SERVICE

203.184.176.X, ESD PRIMARY DATA, HK, DENIAL OF SERVICE
203.197.220.X, GIASBM01.VSNL.NET.IN, IN, SSH
203.198.56.X, IPVPN005150.NETVIGATOR.COM, HK, HTTP ACCESS/NIMDA
203.203.213.X, U213-132.U203-203.GIGA.NET.TW, TW, RCERT BLOCK
203.221.97.150, OPTUS INTERNET, AU, FTP ACCESS
203.228.149.129, CERAGEM, KR, RCERT BLOCK
203.231.32.2, PSINET, KR, DENIAL OF SERVICE
203.236.233.99, KORNET, KR, HTTP ACCESS
203.254.176.176, KOREA TELCOM, KR, RCERT BLOCK
203.73.116.109, DIGITAL UNITED, TW, RCERT BLOCK
203.93.116.X, HENAN NET TRANSON TECH, CN, IIS ACCESS
203.97.100.45, COMPASS COMMUNICATIONS, NZ, HTTP ACCESS
204.101.114.246, WORLDLINX, CA, RCERT BLOCK
204.107.129.2, NORTHTECH COMPUTER, US, SSH
204.107.69.158, TILLAMOOK COUNTY OR, US, SSH
204.210.21.250, SERVICECO LLC, US, SSH
204.210.230.88, ROAD RUNNER, US, DENIAL OF SERVICE
204.233.139.64, ARISTOTLE INTERNET, US, HTTP ACCESS
204.233.41.106, VERIO, INC., US, HTTP ACCESS
204.50.151.72, SAUGEEN TELECABLE, CA, NETBIOS ROOT ACCESS
204.92.252.66, CAPTECH, US, SSH
204.94.172.2, ABSOLUTE DATA PROCESSING, US, MS SQL ROOT ACCESS
205.162.200.11, US SPRINT, US, WU-FTP ACCESS
205.232.30.252, NYSERNET/THE ROSS SCHOOL, US, HTTP ACCESS
205.246.110.136, MURTHA CULLINA RICHTER, US, DENIAL OF SERVICE
205.253.113.100, MACRO COMPUTER SYSTEMS, US, HTTP ACCESS
205.253.200.163, GILLETTE GLOBAL, US, HTTP ACCESS
206.100.84.78, THE NETWORK GROUP, US, SSH
206.104.231.8, ACOOLNET REESE COMPUTER, US, SSH
206.131.240.105, MINERVA NETWORK, US, DENIAL OF SERVICE
206.132.18.210, LOCALEYES CORP., US, SSH ROOT ACCESS
206.142.53.21, IBS, US, SSH
206.170.35.167, PAC BELL, US, ACCESS
206.218.158.90, LOUISIANA DEPT OF EDUCATION, US, NETBIOS ROOT ACCESS
206.252.192.196, STEALTH COMMUNICATIONS, US, IRC ROOT ACCESS
206.50.191.131, ON-RAMP TECHNOLOGIES, US, SSH
206.80.4.165, HOOKED INC., US, HTTP ROOT ACCESS
207.103.151.226, LIFE INSTRUCTORS, US, RCERT BLOCK
207.105.0.134, SHANGHAI COMPUTER LAB, US, SSH
207.124.73.132, CABLE & WIRELESS, TO, RCERT BLOCK
207.139.195.169, COMMUNICATION SCIENCE IMPACT, CA, DENIAL OF SERVICE
207.153.8.152, OA INTERNET, CA, MSTREAM
207.172.7.69, RCN CORP, US, RCERT BLOCK
207.173.156.247, RELIANET, US, HTTP ACCESS
207.174.207.177, WWW.EXPEDIOWARE.COM, US, ADWARE
207.188.7.125, WWW.REAL.COM, US, ADWARE

207.188.7.131, REALNETWORKS, INC., US, FTP ACCESS
207.213.220.70, PACIFIC BELL, US, HTTP ACCESS
207.228.236.26, BN2B.SUPERB.NET, US, SMTP ATTEMPTED DOS
207.229.143.40, ENTERACT, US, SSH
207.229.143.42, ENTERACT, US, SSH
207.243.40.X, MEDIA GENERAL, US, UDP BOMB ATTEMPT
207.244.116.63, RHYTHMIX, INC., US, HTTP AND PORT 2492 GROOVE
207.245.249.150, AT&T CANADA TELECOM SERVICE, CA, DENIAL OF SERVICE
207.246.124.10, WWW.VX2.CC, CC, ADWARE
207.50.158.148, OHIO ONLINE, US, SSH
207.68.183.61, MSN, US, FTP ACCESS
207.71.87.121, UPRD, US, HTTP ACCESS
207.8.144.64, WWW.FLASHTRACK.COM, US, ADWARE
208.137.67.66, BERLIN ELEMENTARY SCHOOL, US, FTP
208.147.89.87, WWW.NETZIP.COM, US, ADWARE
208.177.55.195, XO COMMUNICATIONS, US, RCERT BLOCK
208.177.85.186, XO COMMUNICATIONS, US, RCERT BLOCK
208.178.185.81, DALE BARON, US, FTP ACCESS
208.184.219.243, KEN DILULLO, US, SSH
208.184.56.220, INDULGE.COM, US, SSH
208.185.111.19, IJS SOLUTIONS, US, SSH
208.185.211.71, EZULA.COM, US, ADWARE
208.215.68.X, WWW.BROADCAST.NET, US, ADWARE
208.231.0.100, SKYNETWEB, US, SSH
208.242.37.60, SANDPIPER NETWORKS, US, SSH
208.255.111.214, WWW.ANNOTATE.NET, US, ADWARE
208.45.250.203, QWEST COMMUNICATIONS, US, RCERT BLOCK
208.46.68.212, CARD MASTER SYSTEMS, US, RCERT BLOCK
208.63.169.191, BELLSOUTH, US, HTTP ACCESS
209.11.45.139, WHENU.COM, US, ADWARE
209.128.161.241, 209-128-161-241.DIAL-UP.IPA.NET, US, ACCESS
209.128.45.135, NEWTEL COMMUNICATIONS, CA, ACCESS
209.132.193.8, WWW.GOHIP.COM, US, ADWARE
209.132.218.74, WWW.INTERNETFUEL.COM, US, ADWARE
209.132.232.101, BUDDHA.RBMAILSOURCE.COM, US, SMTP ATTEMPTED DOS
209.133.93.172, ABOVENET COMMUNICATIONS INC., US, FTP ACCESS
209.137.96.252, DUTCHESS COUNTY COMMUNITY COLLEGE, US, NIMDA
209.142.128.X, CENTURY TELEPHONE, US, RCERT BLOCK
209.155.34.66, COMPUNET BUSINESS SYSTEMS, US, SSH
209.167.239.13, OUT3.RAPID-E.NET, CA, SMTP ATTEMPTED DOS
209.167.239.15, OUT5.RAPID-E.NET, CA, SMTP ATTEMPTED DOS
209.167.79.133, MEDIA SYNERGY INC., CA, SMTP ATTEMPTED DOS
209.171.43.18, ISTAR INTERNET, CA, FTP ACCESS
209.172.185.26, ALEXIAN-1.MC.NET, US, NCP PORT 524
209.176.3.45, AMERICAN DATA SERVICE, US, DENIAL OF SERVICE
209.191.149.145, THE ISLAND ECN, INC., US, DENIAL OF SERVICE

209.2.173.2, PIX.NYCHHC.ORG, US, NCP PORT 524
209.202.187.15, EXODUS COMMUNICATIONS, US, DENIAL OF SERVICE
209.207.151.161, WWW.SPEEDBIT.COM, IL, ADWARE
209.21.27.219, SCOTT EIGENHUIS, US, HTTP ACCESS
209.21.37.230, SYNERGISTIC E-SERVICES, US, DENIAL OF SERVICE
209.211.205.41, LCI INTERNATIONAL, US, HTTP ACCESS
209.212.210.2, NET DIRECT, US, DENIAL OF SERVICE
209.215.94.110, TECHNOLOGY INC, US, HTTP ACCESS
209.235.23.74, INTERLIANT, US, SSH
209.237.158.46, WORLD WIDE INTERNET PUBLISHING, US, PORT 555 ACCESS
209.242.130.150, LEMON GROVE SCHOOL DISTRICT, US, NIMDA
209.245.72.245, LEVEL3 COMMUNICATIONS, US, DENIAL OF SERVICE
209.247.41.30, WWW.ALEXA.COM, US, ADWARE
209.249.147.83, ABOVENET COMMUNICATIONS INC., US, FTP ROOT ACCESS
209.27.251.224, NEWDOTNET.NET, US, ADWARE
209.27.3.50, ZEBEC DATA SYSTEM, US, SSH
209.60.70.7, ABLE.NETTEXAS.NET, US, RCERT BLOCK
209.69.30.5, VERIO, INC., US, HTTP ACCESS
209.73.225.11, WWW.CYDOOR.COM, IL, ADWARE
209.79.69.1, ORANGE COUNTY DEPT OF EDUCATION, US, ACCESS
209.83.138.66, SAVVIS COMMUNICATIONS, US, HTTP ACCESS
209.83.193.13, INTERTEK, US, RCERT BLOCK
209.83.8.241, PROGRESSIVE TECHNOLOGIES, US, SSH ACCESS
210.106.227.122, KORNIC, KR, HTTP ACCESS
210.111.51.12, SETRI MICRO SYSTEMS, KR,
210.114.220.31, ONSE TELECOM, KR, PORT 500 ISAKMP
210.12.217.51, JINAN NETWORK COMMUNICATIONS, CN, RCERT BLOCK
210.126.140.32, KOREA TELCOM, KR, RCERT BLOCK
210.14.246.83, JI TONG COMMUNICATIONS, CN, HTTP ACCESS
210.164.135.2, CUSTOM OF CGWNET, CN, HTTP ACCESS
210.171.201.2, AOI SOFTWARE, JP,
210.176.89.18, PACIFIC MILLENNIUM CO LTD, HK, NIMDA
210.178.12.111, TAEWON HIGH SCHOOL, KR, HTTP ACCESS
210.206.42.121, BORANET, KR, DENIAL OF SERVICE
210.22.86.2, SHANGHAI BRANCH, CHINA NET, CN, MS SQL ACCESS
210.22.93.33, LANGAO SMALL SECTION, CN, NETBIOS ROOT ACCESS
210.220.236.250, SAMJINMULSANG, KR, FTP
210.225.32.82, IO.INDEXO.CO.JP, JP, MSTREAM
210.230.200.61, BROOKLANDS CO, JP, SSH
210.244.143.125, ISNET, TW, DENIAL OF SERVICE
210.31.32.8, BEJING INST OF PETRO CHEMICAL TECH, CN, HTTP ACCESS
210.47.144.3, LNEIN-CN, CN, HTTP ACCESS
210.49.71.136, C17529.ROCHD2.QLD.OPTUSNET.CM.AU, AU, ACCESS
210.5.18.92, CHINA GUANGZHOU GUANGTONG, CN, ACCESS
210.70.60.91, PC91.KLCIVS.KL.EDU.TW, TW, ACCESS
210.74.104.221, JITONG COMMUNICATIONS, CN, HTTP ACCESS

210.75.223.9, BICHNET, CN, COLDFUSION ACCESS
210.90.113.120, KUMI GIRLS HIGH SCHOOL, KR, UNKNOWN
210.93.0.11, KRNIC, KR, ROOT ACCESS
210.95.120.251, HWAKWANG TECHNICAL, KR, IIS ACCESS//

BT
NNNN

ADMINISTRATIVE MESSAGE

ROUTINE

R 261302Z AUG 02 ZYB PSN 813583J28

FM FLTINFOWARCEN NORFOLK VA//N3//

TO ALCND

INFO CNO WASHINGTON DC//N6/N614/N6143/N2/N312/N515//
CNO WASHINGTON DC//N6/N614/N6143/N2/N312/N515//
CMC WASHINGTON DC//P/C4I/PLI/CSB/CIS//
CMC WASHINGTON DC//P/C4I/PLI/CSB/CIS//
USCINCSPACE PETERSON AFB CO//J3/J39/J6//
USCINCJFCOM NORFOLK VA//J3/J6//
USCINCJFCOM NORFOLK VA//J3/J6//
CINCLANTFLT NORFOLK VA//N6/N02C/N3/5/7-IW//
CINCPACFLT PEARL HARBOR HI//N3DC/N6/N69//
CINCPACFLT PEARL HARBOR HI//N3DC/N6/N69//
CINCUSNAVEUR LONDON UK//N3/N6/N9//
CINCUSNAVEUR LONDON UK//N3/N6/N9//
COMNAVNETWARCOM NORFOLK VA//N3/N6/N9//
COMNAVNETWARCOM NORFOLK VA//N3/N6/N9//
COMUSNAVCENT//N3/N39/N6//
COMUSNAVCENT//N3/N39/N6//
JTF-CNO WASHINGTON DC//J3/J6/LECIC//
NCTF-CND WASHINGTON DC//N3/N5//
NAVNETSPAOPSCOM DET WASHINGTON DC//N3/N65//
DIRNAVCRIMINVSERV WASHINGTON DC//20/22//
NAVNETSPAOPSCOM GNOC DET NORFOLK VA//N2/N3//
NMCI RNOC NORFOLK VA//N2/N3//
NMCI RNOC SAN DIEGO CA//N2/N3//
MITNOC QUANTICO VA//JJJ//
MITNOC QUANTICO VA//JJJ//
AFIWC LACKLAND AFB TX//EAA//
ACERT FT BELVOIR VA//JJJ//

NRO WASHINGTON DC//COM-EMOC/OSF//
DISA WASHINGTON DC//ASSIST//
DISA WASHINGTON DC//ASSIST//
HQ NORAD COMMAND CTR CHEYENNE MOUNTAIN AFS CO//CC/ND/
    J3/J39//
CMOC CHEYENNE MOUNTAIN AFS CO//NBMC//
CMOC CHEYENNE MOUNTAIN AFS CO//NBMC//

THIS IS A 4 SECTIONED MSG COLLATED BY MDS
UNCLAS //N05239//
PASS TO LAN ADMINISTRATOR, ISSM,
OR TECHNICAL HELP DESK
ALCND 044/02

MSGID/GENADMIN/FLTINFOWARCEN//

SUBJ/NAVCIRT ADVISORY 02-22 - RECOMMENDED IP BLOCK LIST
/PART TWO OF TWO - PART ONE IDENT 261301Z AUG 02//

REF/A/RMG/FLTINFOWARCEN/251301ZJUL2002//

REF/B/RMG/FLTINFOWARCEN/251302ZJUL2002//

REF/C/DOC/CNO/03MAR1998//

NARR/REFS A AND B ARE PARTS ONE AND TWO OF NAVCIRT
ADVISORY 02-20 RECOMMENDED IP BLOCKAGE. REF C IS OPNAVINST
2201.2 WHICH OUTLINES DON POLICY FOR COMPUTER INCIDENT
REPORTING.//
POC/MARI KIRBY/CIV/FLTINFOWARCEN/-/TEL: (757) 417-4187/
(DSN) 537-4187//

RMKS/1. THIS MESSAGE CANCELS REF A AND B.

2. THE FOLLOWING INTERNET PROTOCOL (IP) ADDRESSES HAVE
RECENTLY BEEN REPORTED PROBING AND/OR ATTEMPTING TO ACCESS
NAVY.MIL COMPUTER SYSTEMS. RECOMMEND SYSTEM ADMINISTRATORS
BLOCK THE FOLLOWING IP ADDRESSES AT SYSTEM ROUTERS FOR A
PERIOD TO EXPIRE 30 SEP 2002. THIS RECOMMENDATION DOES NOT
SUPERCEDE USE OF ONE OF THESE SPECIFIC IP ADDRESSES IF
REQUIRED FOR MISSION ACCOMPLISHMENT.
211.105.32.230, KORNET, KR, SSH
211.107.187.10, KORNET, KR, ACCESS
211.114.0.252, KORNET, KR, PORT 515
211.114.147.58, SEMYUNG UNIV, KR, ACCESS
211.120.117.39, YUTOPIA-NET, JP, ICMP FLOOD

211.141.65.4, CHINA MOBILE COMMUNICATIONS, CN, FTP
211.159.100.39, GSNET, CN, HTTP ACCESS
211.174.127.148, MOUMNET, KR, HTTP DOS
211.199.180.226, KOREA TELCOM, KR, MS SQL
211.20.47.138, CHUNGHWA TELECOM, TW, PORTS 6112, 1524
211.201.134.178, HANARO TELECOM, KR, MS SQL ROOT ACCESS
211.206.127.64, HANARO TELECOM, KR, DENIAL OF SERVICE
211.209.215.100, HANANET, KR, RCERT BLOCK
211.217.25.162, KOREA TELCOM, KR, ACCESS
211.218.149.27, CENTRAL DATA COMMUNICATION, KR, MSTREAM
211.226.221.80, KOREA TELCOM, KR, DENIAL OF SERVICE
211.230.84.18, NIC.OR.KR, KR, SSH
211.239.86.2, CLOUD 9, KR, MS SQL ACCESS
211.37.214.40, CHINA UNITED TELECOMMUNICATIONS, CN, FTP ACCESS
211.43.203.64, NPIX, KR, HTTP ACCESS
211.47.68.113, TTNT, KR, MS SQL
211.5.112.39, YOKOHAMA MEDIA CORP, JP, SSH
211.62.112.100, HYEKWANG INFORMATION TELCOM, KR, SSH
211.62.54.163, KORNET, KR, FTP
211.62.59.10, KORNET, KR, DENIAL OF SERVICE
211.74.207.171, KAOSIUNGDP-NET, TW, FTP ACCESS
211.75.161.36, CHUNGHWA TELECOM, TW, DENIAL OF SERVICE
211.95.73.166, SHANGHAI IDC, CN, ACCESS
211.96.252.251, GD-DONGGUAN, CN, WEB HACK
211.99.6.37, TELETRON, CN, HTTP ACCESS
212.1.136.26, TELINCO INTERNET, GB, FTP ACCESS
212.1.140.146, TELINCO INTERNET, GB, FTP ACCESS
212.1.148.39, TELINCO INTERNET, GB, FTP ACCESS
212.107.153.252, MADGE.NET, GB, ROOT ACCESS
212.120.100.219, BENELUX, NL, DENIAL OF SERVICE
212.121.162.9, FLUXUS FRANCENET, FR, SSH
212.135.130.131, COMPUTER SOLUTIONS, GB, DENIAL OF SERVICE
212.144.129.X, ARCOR.NET, DE, ACCESS
212.144.130.45, ARCOR.NET, DE, ACCESS
212.16.34.9, VIP EDV DIENSTLEISTUNGEN GMBH, AT, SSH
212.171.146.11, INTERBUSINESS, IT, PORT 6112
212.171.38.117, INTERBUSINESS, IT, IDS MAPPING
212.186.193.239, SUFER.AT, AT, ACCESS
212.188.128.139, SCREAMING FREE ISP, GB, ROOT ACCESS
212.191.70.179, LODZ.PL, PL, ACCESS
212.194.84.216, CLUB-INTERNET.FR, FR, ACCESS
212.198.84.181, LYONNAISE COMMUNICATIONS, FR, SSH
212.211.6.107, UUNET, GB, ROOT ACCESS
212.211.84.6, FRA-TGN-OYE-VTY6.AS.WCOM.NET, US, DENIAL OF SERVICE
212.23.166.113, RFO FRENCH NETWORK, FR, FTP ACCESS
212.242.94.183, CYBERCITY INTERNET, DK, MS SQL ROOT ACCESS

212.40.5.89, DATACOMM, CH, RCERT BLOCK
212.42.96.33, UNIX.OFFICE.ELCAT.KG, KG
212.67.238.20, TRA-IBK-ACHAMER, AT, WU-FTP ACCESS
212.68.238.102, BRUTELE.BE, BE, ACCESS
212.74.122.6, APPLENET, UK, SSH
212.77.192.44, INTERNET QATAR, QA, HTTP ACCESS
212.93.151.47, ROMANIA DATA SYSTEMS, RO, HTTP ACCESS
213.1.100.120, BT INTERNET, GB, PORT 2000 ROOT ACCESS
213.1.156.168, BT-IMSNET, GB, FTP ACCESS
213.1.92.45, BT INTERNET, GB, FTP ACCESS
213.121.116.143, BT PUBLIC INTERNET SERVICE, GB, FTP BOUNCE, IDS MAPPING
213.121.253.106, ENGLISH ARCHITECTURAL LTD, UK, SSH
213.122.177.154, BRITISH TELECOMMUNICATIONS, UK, HTTP ACCESS
213.122.83.54, BT-IMSNET, GB, FTP ACCESS
213.132.139.6, TVD INTERNET, BE, HTTP ACCESS
213.142.95.35, SNAPP SEARCH AS, NO, SSH
213.143.122.127, MAXEXP.COM, US, LOPSEARCH.EXE
213.151.134.135, KVALITO, NO, HTTP ACCESS
213.175.32.246, CZ FASTNER, CZ, HTTP ACCESS
213.20.26.34, MEDIAWAYS, DE, FTP ACCESS
213.219.72.166, ESTONIAN TELEPHONE, EE, HTTP EXPLOITS
213.224.86.206, D5E056CE.KABEL.TELENET.BE', BE, FTP ACCESS
213.23.36.50, MANNESMANN ARCOR AG & CO, DE, FTP ACCESS
213.23.70.131, ARCOR.NET, DE, ACCESS
213.233.126.51, INTERNET CLUB, RO, BACKDOOR PORT 6194
213.237.78.10, WORLD ONLINE DENMARK, DK, FTP ROOT ACCESS
213.248.107.10, ALPHA.KAZAA.COM, NL, P2P
213.33.153.14, SOVINTEL.NET, RU, FTP
213.47.176.35, GRAZ-CUSTOMER-CABLE, AT, FTP ACCESS
213.6.192.78, PPPOOL.DE, DE, ACCESS
213.64.240.91, TELIA NETWORK SERVICES, SE, HTTP ACCESS
213.67.184.35, TELIA NETWORK SERVICES, SE, HTTP DOS ATTEMPT
213.76.215.196, PA196.GORZOW.SDI.TPNET.PL, PL, MS SQL
213.82.195.130, INTERBUSINESS, IT, SSH
216.111.111.38, SHOCKING.COM, US, SMTP & PORT 113 KAZIMAS WORM
216.119.133.X, WORLD TRADE NETWORK, US, ATTEMPTED DOS
216.160.91.57, DIRECTWEB, US, SSH
216.167.113.X, WWW.SPEEDBIT.COM, IL, ADWARE
216.167.2.X, WALNUT ACRES ORGANIC FARMS, US, SSH ROOT ACCESS
216.167.25.146, WWW.SPEEDBIT.COM, IL, ADWARE
216.167.27.38, MEDIA VISUAL HITECH, HK, SSH
216.167.51.189, WWW.SPEEDBIT.COM, IL, ADWARE
216.190.164.244, NORTHWEST TELEPHONE, US, SSH
216.190.255.220, WASATCH HOSTING, US, RCERT BLOCK
216.194.70.4, TERABYTE DOT COM, CA, WORM EXPLOIT ORIGINATOR

216.20.161.58, FASTPOINT COMMUNICATIONS, US, SSH ACCESS
PASS TO LAN ADMINISTRATOR, ISSM,
OR TECHNICAL HELP DESK
ALCND 044/02

MSGID/GENADMIN/FLTINFOWARCEN//

SUBJ/NAVCIRT ADVISORY 02-22 - RECOMMENDED IP BLOCK LIST
216.204.94.107, NET RESOURCE, US, RCERT BLOCK
216.206.101.2, LEBANON CABLEVISION, US, SSH
216.207.32.194, MUSICIAN'S FRIEND, US, SMTP
216.207.80.X, WWW.WEB3000.COM, US, ADWARE
216.211.204.176, FIRSTGATE.NET, US, ACCESS
216.232.194.215, NEWTON CONSUMER DSL, CA, RCERT BLOCK
216.232.36.98, TRINITY CONSUMER ADSL, CA, SOCKS PORT 1080
216.233.43.250, THYTHMS NETCONNECTIONS, US, IIS ACCESS
216.234.161.X, WWW.GNUTELLA.COM, US, P2P
216.234.42.4, NETWORK CONNECTION, CA, HTTP ACCESS
216.237.145.44, DELTA ISP, US, RCERT BLOCK
216.239.175.36, BAUER COMMUNICATIONS, US, PORT 443 SSL ROOT ACCESS
216.242.90.92, SUITEBUILD.COM, US, WEB HACK
216.252.165.211, INTERPACKET GROUP, US, HTTP ACCESS
216.254.144.X, PRIMUS, CA, SMTP
216.28.108.51, VENTURE HOSTING, US, SSH
216.37.13.152, WWW.RADIATE.COM, US, ADWARE
216.40.211.23, EVERYONES INTERNET, US, SSH
216.52.126.X, PERFORMANCE-ATT.WDC.PNAP.NET, US, ATTEMPTED DOS
216.52.223.4, PNAP.NET, US, ATTEMPTED DOS
216.52.41.68, PNAP.NET, US, ATTEMPTED DOS
216.57.13.125, ONSIGHT ACCESS, CA, RCERT BLOCK
216.60.120.33, ST. LOUIS CHURCH, US, FTP ACCESS
216.61.164.89, CREATIVE.COM, US, ADWARE
216.65.4.2, HOSTCENTRIC.COM, US, SSH
216.7.10.28, ARTMATRIX, US, SSH
216.7.148.251, TERRACOM, US, SSH
216.77.166.161, BELLSOUTH, US, HTTP ACCESS
216.77.192.44, INTERNET QATAR, QA, HTTP ACCESS
216.79.118.174, BELLSOUTH, US, RCERT BLOCK
216.86.202.101, MM INTERNET, CA, RCERT BLOCK
216.93.104.34, VOYAGER.NET, US, HTTP ACCESS
217.0.101.124, T-DAILIN.NET, DE, ACCESS
217.11.254.37, ABO.CZ, CZ, ACCESS
217.119.193.199, EASTERN GRAPHICS, DE, RCERT BLOCK
217.120.8.70, ATHOME BENELUX NETWORK, NL, SSH
217.128.160.194, FRANCE TELECOM, FR, RCERT BLOCK
217.128.241.240, 1P2000-ADSL-BAS, FR, FTP ACCESS

217.128.67.54, FRANCE TELECOM, FR, FTP ACCESS
217.128.97.129, FRANCE TELECOM, FR, PRINT SERVER
217.136.156.90, SKYNET.BE, BE, ACCESS
217.156.116.X, CANAD SYSTEMS INTERNET, RO, SSH
217.195.194.101, TEKLAN, TR, RCERT BLOCK
217.225.109.X, T-DAILIN.NET, DE, ACCESS
217.225.150.X, DEUTSCHE TELEKOM AG, DE, FTP ACCESS
217.225.223.X, DEUTSCHE TELEKOM AG, DE, HTTP ACCESS
217.226.197.X, DEUTSCHE TELEKOM AG, DE, FTP ACCESS
217.226.205.X, DEUTSCHE TELEKOM AG, DE, FTP ACCESS
217.227.49.X, T-DAILIN.NET, DE, ACCESS
217.229.172.X, T-DAILIN.NET, DE, ACCESS
217.230.10.X, T-DAILIN.NET, DE, ACCESS
217.230.30.X, T-DAILIN.NET, DE, ACCESS
217.231.193.X, T-DAILIN.NET, DE, ACCESS
217.231.195.X, IPCONNECT.DE, DE, ACCESS
217.231.197.X, IPCONNECT.DE, DE, ACCESS
217.235.76.X, IPCONNECT.DE, DE, ACCESS
217.57.19.X, CDC-COMPUTER DATA CONTROL, IT, FTP ACCESS
217.59.102.X, PANTAPUBLIROMA, IT, RCERT BLOCK
217.77.130.110, LUNA.NL, NL, SSH
217.81.153.X, T-DAILIN.NET, DE, ACCESS
217.81.22.X, T-DAILIN.NET, DE, ACCESS
217.81.235.X, T-DAILIN.NET, DE, ACCESS
217.81.249.X, T-DAILIN.NET, DE, ACCESS
217.81.250.X, T-DAILIN.NET, DE, ACCESS
217.84.23.X, T-DAILIN.NET, DE, ACCESS
217.84.26.X, T-DAILIN.NET, DE, ACCESS
217.87.87.X, DEUTSCHE TELEKOM, DE, ANON FTP COMPROMISE
217.96.212.X, TYCHY-SDI, PL, RCERT BLOCK
217.98.50.X, OHO-INTERNET, PL, RCERT BLOCK
218.146.254.X, KOREA TELCOM, KR, MSTREAM
218.202.40.X, CHINA MOBILE COMMUNICATIONS, CN, RCERT BLOCK
218.55.100.X, HANARO TELECOM, KR, FTP
218.7.3.X, CHINANET, CN, HTTP ACCESS
24.102.117.98, CPE005DAB4CD3A.CPE.NET.CABLE.ROGERS.COM, CA, BOTNET
24.120.41.5, COMMUNITY CABLE, US, RCERT BLOCK
24.147.182.173, H00D05905DE47.NE.CLIENT2.ATTBI.COM, US, MS SQL
24.156.119.72, ROGERS@HOME, CA, FTP ROOT ACCESS
24.163.20.166, GSO163-20-166.TRIAD.RR.COM, US, MS SQL
24.165.46.141, ROAD RUNNER, US, RCERT BLOCK
24.167.6.100, SERVICECO LLC - ROADRUNNER, US, CODE RED WORM
24.168.191.153, AT&T BROADBAND, US, DENIAL OF SERVICE
24.198.36.204, ROAD RUNNER, US, RCERT BLOCK
24.202.237.38, VIDEOTRON LTEE, CA, HTTP ACCESS
24.218.59.16, SERVICECO LLC - ROADRUNNER, US, TELNET ROOT ACCESS

24.228.24.8, CABLEVISION SYSTEMS, US, FTP ACCESS
24.3.47.253, @HOME NETWORK, US, HTTP ACCESS
24.42.198.248, ROGERS@HOME, CA, FTP ROOT ACCESS
24.43.173.59, ROGERS@HOME, CA, FTP ROOT ACCESS
24.64.93.75, SHAW FIBERLINK, CA, RCERT BLOCK
24.73.44.192, ROAD RUNNER, US, RCERT BLOCK
24.88.1.103, MEDIA 1, US, HTTP ACCESS
24.95.197.77, ROAD RUNNER, US, RCERT BLOCK
38.214.195.27, PSI, US, RCERT BLOCK
4.19.239.3, ORACLE CORPORATION, US, NIMDA
4.33.19.30, EVERETT GOSPEL MISSION, US, FTP ACCESS
4.35.254.110, GENUITY, US, SSH
4.48.114.90, BBN PLANET CORP, US, HTTP ACCESS
61.128.97.X, CHINANET, CN, HTTP ACCESS
61.133.102.X, SHANDONG TELECOM, CN, HTTP ACCESS
61.133.165.X, SHANDONG TELECOM, CN, HTTP ACCESS
61.133.87.X, YANTAI LONGKOU CITY TELECOM, CN, ACCESS
61.134.3.X, SNXIAN, CN, HTTP ACCESS
61.134.4.X, SNXIAN, CN, SSH
61.135.14.X, CHINANET, CN, HTTP ACCESS
61.136.11.X, ZHENGLIAN-NET, CN, HTTP ACCESS
61.138.232.X, CHINANET, CN, IIS ACCESS
61.139.42.X, CHINANET, CN, HTTP ACCESS
61.139.59.X, CHINANET, CN, HTTP ACCESS
61.140.23.X, CHINANET, CN, HTTP ACCESS
61.142.242.X, CHINANET, CN, IIS ACCESS
61.144.176.X, CHINA TELECOM, CN, HTTP ACCESS
61.144.231.X, CHINANET, CN, HTTP ACCESS
61.150.176.X, CHINA TELECOM, CN, HTTP ACCESS
61.150.49.X, SNXIAN, CN, HTTP ACCESS
61.152.129.X, CAPITAL ONLINE, CN, HTTP ACCESS
61.152.210.X, SHANGHAI DIGITALCOM, CN, KLEZ ATTEMPTS
PASS TO LAN ADMINISTRATOR, ISSM,
OR TECHNICAL HELP DESK
ALCND 044/02

MSGID/GENADMIN/FLTINFOWARCEN//

SUBJ/NAVCIRT ADVISORY 02-22 - RECOMMENDED IP BLOCK LIST
61.165.193.X, CHINANET, CN, ACCESS
61.165.195.X, CHINANET, CN, ACCESS
61.169.144.X, CHINANET, CN, HTTP ACCESS
61.169.168.X, CHINANET, CN, ACCESS
61.171.18.X, CHINANET, CN, ROOT ACCESS
61.171.86.X, CHINANET, CN, ATTEMPTED DOS (FTP)
61.171.86.X, CHINANET, CN, ATTEMPTED DOS (FTP)

61.171.93.X, CHINANET, CN, NETBIOS ROOT ACCESS
61.171.93.X, CHINANET, CN, HTTP ACCESS
61.178.24.X, CHINANET, CN, MUTLIDROPPER-CX WORM
61.133.87.X, YANTAI LONGKOU CITY TELECOM, CN, FTP
61.179.119.X, CHINANET, CN, SUNRPC
61.183.18.X, DAWU MIDDLE SCHOOL, CN, PORT 500 ISAKMP
61.187.197.X, CHINANET, CN, HTTP ACCESS
61.200.81.X, AKAMAI TECHNOLOGIES, JP, RCERT BLOCK
61.73.151.X, KOREA TELCOM, KR, PORT 3389 NT TERMINAL SERVER
61.73.62.X, KOREA TELECOM, KR, SSH
61.79.170.X, KOREA TELCOM, KR, DENIAL OF SERVICE
61.9.96.X, BOHOL QUALITY CORP, PH, PORT 5101 TALARIAN
61.98.227.X, KORNET, KR, RCERT BLOCK
62.109.68.X, HANSENET.DE, DE, ACCESS
62.109.68.X, HANSENET.DE, DE, ACCESS
62.109.77.X, B077099.ADSL.HANSENET.DE, DE, ACCESS
62.109.78.X, HANSENET.DE, DE, ACCESS
62.109.79.X, HANSENET.DE, DE, ACCESS
62.109.81.X, HANSENET.DE, DE, ACCESS
62.109.82.X, HANSENET.DE, DE, ACCESS
62.110.117.X, CIBRA-PUBBLICITA-SRL, IT, SSH ACCESS
62.110.118.X, E-CUBE, IT, PORT 500 ISAKMP
62.122.74.X, GALACTICA.IT FLATRATE USERS, IT, ACCESS
62.140.73.X, EG-NMC, EG, HTTP ACCESS
62.153.209.X, MAIL.21-GRAD.DE, DE, FTP
62.154.210.X, ALFA-NET, DE, ACCESS
62.158.33.X, DEUTSCHE TELEKOM, DE, FTP ACCESS
62.159.145.X, MULTIMEDIA IN BAYERN AG, DE, DENIAL OF SERVICE
62.188.131.187, UUNET.UU.NET, GB, ACCESS
62.212.98.116, NERIM-ADSL-FT-20010912, FR, FTP ACCESS
62.214.53.213, FONI.NET, DE, ACCESS
62.226.148.192, DEUTSCHE TELEKOM, DE, FTP ACCESS
62.227.11.23, DEUTSCHE TELEKOM ONLINE, DE, DENIAL OF SERVICE
62.229.59.15, GLOBAL ONE, SE, HTTP ACCESS
62.236.118.98, PLANETMEDIA, FI, HTTP ACCESS
62.243.42.88, TDC-ADSL-USERS, DK, FTP ACCESS
62.254.134.90, NTL INTERNET, GB, FTP ACCESS
62.27.222.53, CIBRA-PUBBLICITA-SRL, IT, SSH ROOT ACCESS
62.47.24.X, TELEKOM.AT, AT, ACCESS
62.62.189.250, 9TEL.NET, FR, ACCESS
62.62.189.70, 9TEL.NET, FR, ACCESS
62.7.112.18, BT INTERNET, GB, FTP ACCESS
62.7.24.186, BT INTERNET, GB, FTP ACCESS
62.7.244.126, BRITISH TELECOMMUNICATIONS, GB, ROOT ACCESS
62.7.49.63, BT-IMSNET, GB, FTP ACCESS
62.73.5.136, NETWORK COMM, FR, SSH

62.98.208.112, WIND-FREE-33, IT, ACCESS
63.107.113.156, FREESTATELOTTO.COM, US, HTTP ACCESS
63.124.119.143, ACER AMERICA CORP, US, HTTP ACCESS
63.126.90.3, PACIFIC BELL, US, DENIAL OF SERVICE
63.147.172.170, QWEST COMMUNICATIONS, US, RCERT BLOCK
63.193.108.219, PBI.NET, US, MS SQL
63.193.155.218, ADSL BASIC, US, HTTP EXPLOITS
63.196.113.83, PACIFIC BELL, US, DENIAL OF SERVICE
63.200.89.50, DOUGLASS JONES, US, DENIAL OF SERVICE
63.202.85.24, UUNET, US, DENIAL OF SERVICE
63.208.149.6, E-SYNC NETWORKS, US, RCERT BLOCK
63.209.12.191, LEVEL 3, US, DENIAL OF SERVICE
63.224.241.249, INCLUSION INC, US, MS SQL
63.240.211.149, AT&T FIRSTGOV SEARCH, US, ACCESS
63.250.132.4, INFONET SERVICES CORP, US, ACCESS
63.89.178.226, ANDERSON MACHINING, US, RCERT BLOCK
63.92.15.15, TSI BROADBAND, US, RCERT BLOCK
64.0.246.102, CONCENTRIC NETWORK , US, SSH
64.124.36.229, SPIV TECHNOLOGIES, US, SSH
64.15.202.143, GLOBAL CENTER, US, SSH
64.152.128.117, LEVEL 3, US, SSH
64.192.85.133, TELOCITY, US, RCERT BLOCK
64.21.68.162, NET ACCESS CORP, US, SSH
64.218.62.68, FMC CORP, US, RCERT BLOCK
64.23.0.100, SKYNETWEB, US, SSH
64.23.60.206, SKYNETWEB, US, SSH
64.230.56.206, NEXXIA HSE, CA, FTP ROOT ACCESS
64.26.141.56, WWW.WEBENHANCER.COM, CA, ADWARE
64.37.114.92, WWW.TWISTEDHUMOR.COM, US, ADWARE
64.4.14.250, MS HOTMAIL, US, SSH ROOT ACCESS
64.41.22.204, VERZA-NET, NL, IIS ACCESS
64.42.18.114, RENO CARSON MESSENGER SERVICE, US, CODE RED WORM
64.49.144.1, NETSTAT EXPRESS, US, SSH
64.52.128.117, EUREKA BROADBAND, US, SSH
64.59.20.27, OPNET SYSTEMS, US, WEB TRAVERSAL
64.67.4.162, NETWORK ACCESS SOLUTIONS, US, FTP ACCESS
64.70.22.156, LAOUTBOUND3.JACKPOT.COM, US, ROOT ACCESS
64.70.38.178, WWW.BRILLIANTDIGITAL.COM, US, ADWARE
64.86.192.68, TELEGLOBE , US, RCERT BLOCK
64.91.53.51, CENTURY TELEPHONE, US, FTP ACCESS
64.94.219.113, NETPALNOW.COM, US, ADWARE
64.94.33.X, PNAP.NET, US, ATTEMPTED DOS
64.94.89.X, WWW.GATOR.COM, US, ADWARE
65.1.187.71, HOME NETWORK, US, FTP ACCESS
65.116.89.240, DSS.GOTDNS.ORG, US, BOTNET
65.12.143.67, @HOME NETWORK, US, TELNET ROOT ACCESS

65.121.237.200, WWW.HOTBAR.COM, US, ADWARE
65.121.97.139, ALLURE, US, RCERT BLOCK
65.166.1.2, SHADOW INFORMATION SERVICES, US, FTP ACCESS
65.174.143.170, BK MEDIA, US, TELNET
65.196.90.10, ROKU TECHNOLOGIES, US, MSTREAM
65.202.85.24, UUNET, US, SMTP ATTEMPTED DOS
65.214.43.159, NELSON.TECHTARGET.COM, US, SMTP ATTEMPTED DOS
65.223.127.153, ROCKLIFFE, US, SMTP ATTEMPTED DOS
65.32.52.171, ROAD RUNNER, US, RCERT BLOCK
65.64.219.1, SOUTHWESTERN BELL, US, DENIAL OF SERVICE
65.66.19.0, POOL, US, RCERT BLOCK
65.80.225.69, BELLSOUTH, US, CODE RED WORM
65.81.102.179, BELLSOUTH, US, RCERT BLOCK
65.89.41.161, WWW.LOP.COM, US, LOPSEARCH.EXE
65.89.42.150, TRINITY ACQUISITIONS, US, LOPSEARCH.EXE
65.89.43.186, PULSE WEB VENTURES, US, LOPSEARCH.EXE
66.119.41.70, WWW.NETSETTER.COM, US, ADWARE
66.121.74.20, STARSTREAM COMMUNICATIONS, US, DENIAL OF SERVICE
66.130.78.202, VIDEOTRON LTEE, CA, RCERT BLOCK
66.134.37.194, H-66-134-37-194.HSTQTX02.COVAD.NET, US, FTP
66.136.215.114, ASSURED TRAFFIC, US, RCERT BLOCK
66.2.190.103, INTERNET ALLEGIANCE, US, SSH
66.20.189.35, BELLSOUTH, US, DENIAL OF SERVICE
66.21.164.122, ROAD RUNNER, US, RCERT BLOCK
66.24.29.126, ROAD RUNNER, US, RCERT BLOCK
66.240.171.42, BROADSPIRE, CA, RCERT BLOCK
66.65.25.155, ROAD RUNNER, US, RCERT BLOCK
66.76.4.17, TCA INTERNET, US, ROOT ACCESS
66.88.129.150, XO COMMUNICATIONS, US, RCERT BLOCK
67.209.104.46, UUNET, US, RCERT BLOCK
68.65.55.36, ADELPHIA, US, MS SQL ACCESS
68.7.255.154, IP68-7-255-154.SD.SD.COX.NET, US, IIS PROBES
68.81.173.58, COMCAST CABLE, PA, RCERT BLOCK
68.82.228.65, COMCAST CABLE, US, RCERT BLOCK
80.11.0.X, FRANCE TELECOM, FR, RCERT BLOCK
80.11.152.189, WANNADOO, FR, FTP ACCESS
80.11.239.118, 1P2000-ADSL-BAS, FR, RCERT BLOCK
80.11.35.189, WANNADOO, FR, RCERT BLOCK
80.128.0.X, DEUTSCHE TELEKOM, DE, RCERT BLOCK
80.13.0.X, FRANCE TELECOM, FR, RCERT BLOCK
80.13.93.X, WANNADOO, FR, ROOT ACCESS
80.131.27.X, T-DIALIN.NET, DE, ACCESS
80.131.91.X, T-DIALIN.NET, DE, ACCESS
80.133.88.X, DTAG-DIAL16, DE, FTP ACCESS
80.134.167.X, IPCONNECT.DE, DE, ACCESS
80.134.249.X, T-DAILIN.NET, DE, ACCESS

80.134.31.X, T-DIALIN.NET, DE, ACCESS
80.136.0.X, DEUTSCHE TELEKOM, DE, RCERT BLOCK
80.143.181.X, T-DIALIN.NET, DE, ACCESS
80.143.182.X, T-DAILIN.NET, DE, ACCESS
80.200.148.X, SKYNET.BE, BE, ACCESS
80.247.208.X, 31337.VEDROMO.ORG, NL, DENIAL OF SERVICE
80.26.13.125, RIMA, ES, PORT 443 SSL
80.3.204.233, NTL INTERNET, GB, RCERT BLOCK
80.56.161.148, NL-CHELLO, NL, FTP ACCESS
80.62.3.213, TELEDANMARK-ADSL-USERS, DK, SSH
80.8.6.47, WANADOO, FR, RCERT BLOCK
80.81.107.46, SKYPOINT, ES, ACCESS

3. NAVCIRT RECOGNIZES IT-21/GOTS DELTA UNITS ARE UNABLE TO COMPLETE
THESE RECOMMENDED IP BLOCKS AT THEIR BORDER ROUTERS DUE TO PROGRAM
OF RECORD LIMITATIONS. FLEET NOCS CAN AND WILL BLOCK IP'S FOR AFLOAT
UNITS AS REQUIRED. IF UNCERTAIN THAT IP BLOCKS ARE TAKING PLACE,
UNITS MAY CONTACT THEIR SERVICING NOC FOR MORE INFORMATION.

4. IN CASES OF QUESTIONABLE PING/SCAN ACTIVITY, SYSTEM
ADMINISTRATORS ARE URGED TO BLOCK THE SOURCES AS NECESSARY TO
DETER NETWORK MAPPING AND POSSIBLE FOLLOW-ON INTRUSION. IF YOU
HAVE SPECIFIC CONCERNS CONTACT NAVCIRT FOR GUIDANCE.

5. ADDITIONAL NAVCIRT SUPPORT:

A. AS A PREVENTIVE NETWORK SECURITY MEASURE IT IS STRONGLY
RECOMMENDED THAT A FIWC ON-LINE SURVEY (OLS) BE SCHEDULED TO
IDENTIFY KNOWN OR COMMON VULNERABILITIES ON RESIDENT
NETWORKS (NIPRNET/SIPRNET/JWICS). TO REQUEST AN OLS, SEND AN
EMAIL TO OLS@FIWC.NAVY.MIL.
B. TO ENSURE DON WEB SITES ARE IN FULL COMPLIANCE WITH
PUBLISHED DIRECTIVES, FIWC WILL CONDUCT A WEB RISK
ASSESSMENT UPON REQUEST. TO COORDINATE THE ASSESSMENT,
SEND AN EMAIL TO WEB-ASSESSMENT@FIWC.NAVY.MIL.
C. NAVCIRT ADVISORIES ARE ALSO AVAILABLE VIA UNCLAS
ELECTRONIC MAIL. TO RECEIVE NAVCIRT ADVISORIES DIRECTLY TO
.MIL OR .GOV ELECTRONIC MAIL ACCOUNTS, SEND AN E-MAIL TO:
MAJORDOMO@FIWC.NAVY.MIL WITH THE FOLLOWING THREE LINES IN
THE CONTENT OF THE E-MAIL, SUBSCRIBE NAVCIRT-ADV
(FOLLOWED BY YOUR E-MAIL ADDRESS); HELP; END.
D. COMPUTER VIRUSES, TROJAN HORSES, OTHER MALICIOUS CODE
INCIDENTS, KNOWN OR SUSPECTED NETWORK INTRUSIONS AND

OTHER SUSPICIOUS COMPUTER INCIDENTS MUST BE REPORTED TO
NAVCIRT IAW REF A. NAVCIRT OPERATES 24 HOURS A DAY,
SEVEN DAYS A WEEK. IF YOU HAVE QUESTIONS ABOUT THESE OR
ANY OTHER RELATED ISSUES, PLEASE CONTACT NAVCIRT THROUGH
ANY OF THE FOLLOWING MEANS:
- MAILING ADDRESS: DEPARTMENT OF THE NAVY, COMMANDING
OFFICER, FLEET INFORMATION WARFARE CENTER, ATTN:
NAVCIRT, 2555 AMPHIBIOUS DRIVE, NORFOLK, VA 23521-3225
- OFFICIAL MESSAGE: FLTINFOWARCEN NORFOLK VA/N3/N31/
- PHONE: COML (757) 417-4024, (DSN) 537-4024, (DRSN) 521-6123
- NAVCIRT HOTLINE: 1-888-NAVCIRT OR 1-888-628-2478
- UNCLASSIFIED FAX: (757) 417-4031
- CLASSIFIED FAX: (757) 417-4020
- EMAIL: NAVCIRT@FIWC.NAVY.MIL
     NAVCIRT@FIWC.NAVY.SMIL.MIL
- WEBSITES: WWW.FIWC.NAVY.MIL
- WWW.FIWC.NAVY.SMIL.MIL

6. THIS ALCND IS CANCELLED FOR RECORD PURPOSES 30 SEP 02.//

BT
NNNN