~~SECRET~~

National Reconnaissance Office

24 April 1997
NROD 61-1
Information Technology

SUBJECT: NRO Internet Policy

A. PURPOSE. To provide clear guidance on the use of National Reconnaissance Office (NRO) government-provided Internet accounts by NRO personnel, government and contractors, both in the workplace and at home.

B. SCOPE.

1. This policy applies to NRO-sponsored use of Internet computer services. It provides minimum criteria for such use and does not preclude the Directorates and Program Offices or their designees from imposing further restrictions.

2. All NRO personnel, government and contractor, having access to classified/protected information are entitled to use that information only as authorized and necessary in the performance of their jobs. Accessing networks and/or information systems such as the Internet by way of a private account does not relieve the user of the responsibility to avoid unauthorized disclosures. Classified, Privacy Act, For Official Use Only, and sensitive data may not be released on the Internet. Unclassified information considered sensitive if acknowledged publicly or revealing of classified information when combined with other data must not be released without review by the Cognizant Security Office (CSO) and the Office of Primary Responsibility (OPR). If the information is to be widely available publicly, such as a speech or a posting to a public electronic bulletin board, and if the information could be construed as official NRO policy or position due to the

CL BY: (b)(3)
CL REASON: 1.5(c)
DECL ON: X1
DRV FROM: NRO SCG 4.0
14 October 1995

~~SECRET~~

individual's position, expertise, or employment, the information must be reviewed and approved by the CSO and OPR.

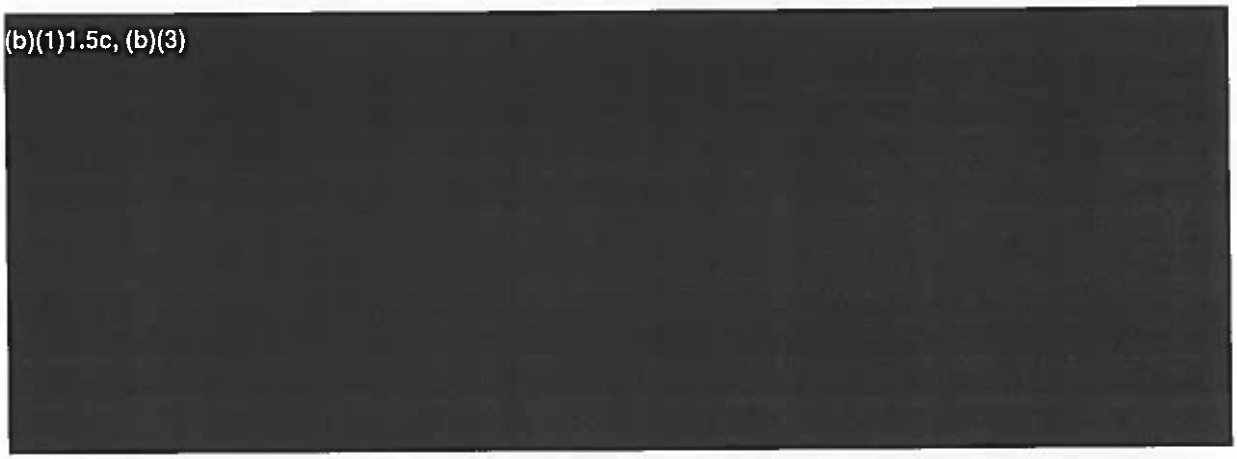
3. The NRO acknowledges the risk of attack against its Internet systems and the potential for inadvertent or unauthorized release of classified information on the Internet. It has deployed and will continue to employ protective mechanisms against external attacks. The NRO relies on each user's compliance with established policy and guidelines to minimize the potential for inadvertent or unauthorized disclosure of information. The Communications Directorate, Information Technology Group (COMM/ITG) will serve as the system administrator providing oversight and maintenance for NRO Internet Services. No Automated Information System (AIS) with access to any classified system or network will have direct access to the Internet (See Automated Information System Security Implementation Manual [AISSIM - 200]).

C. NRO INTERNET SYSTEMS.

1. NRO users will be placed in (b)(1)1.5c, (b)(3) categories/ services.

a. Unclassified/Officially Released. Unclassified/ officially released users are those personnel who are openly announced to the public (e.g., personnel listed in the Department of Defense phone directory). Personnel whose names and positions have been officially released will access the Internet through an open, publicly identified NRO service.

(b)(1)1.5c, (b)(3)



2. Selection of the appropriate Internet service should occur only after discussion with Directorate or Office Senior Management and Program Security.

3. An NRO World Wide Web Home Page exists on the Internet as an official means of disseminating information relating to the NRO. A publication review process exists to verify that all material released on the Internet home page is unclassified and represents the official NRO position.

D. APPROPRIATE USE.

1. Users shall employ the NRO Internet services for official unclassified U.S. Government business only. Users with an unclassified association with the NRO shall not identify other NRO employees except those officially released. Any other identification of NRO personnel requires prior concurrence of the individual involved. Personnel are also cautioned against exposing classified NRO associations through any exchange conducted between NRO Internet services and/or any other Internet service. It is assumed that the Internet services for users with unclassified associations may be traceable to the NRO.

2. Users may not encrypt their data without the express written consent of their sponsoring Directorate or Office Senior Management and their Program Security Officer (PSO).

3. E-mail and Internet accounts will not be shared unless specifically authorized by the Directorate/Program Office in coordination with the PSO. The user is responsible for all activity that takes place on his/her account.

4. No personally-owned hardware or software may be connected to the Internet within a sensitive compartmented information facility without Directorate or Office Senior Management and PSO approval.

E. TRANSFORMATION OF INFORMATION. Users may be authorized by their Directorate or Office Senior Management and PSO to download and upload unclassified programs and textual information between the Internet and other AIS. However, the movement of this information is limited by NRO regulations and policy which prescribe specific precautions to avoid potentially catastrophic virus contamination of NRO-sponsored computer systems. Movement of classified information from any classified system to the Internet is prohibited (See AISSIM - 200).

F. APPROVAL & SECURITY AWARENESS. Written approval from Directorate or Office Senior Management is required to obtain an NRO Internet account. The approving authority and the appropriate PSO are responsible for ensuring that all users read the "NRO Internet Policy" and "NRO Internet User Guidelines" and sign a statement indicating acceptance of the terms. Internet training includes an informational package and a videotape addressing security and privacy on the Internet. As appropriate, updated security awareness briefings will be provided in conjunction with the annual revalidation of Internet accounts. All PSOs and Internet Systems Administrators are required to attend Internet training and any annual briefings.

G. SYSTEM AUDIT. NRO Internet use will be monitored as the NRO deems appropriate. Users will not assume any expectation of privacy on this system. All monitoring activities will be coordinated with COMM/ITG, NRO Office of Security's Facilities and Information Security Division, and the NRO General Counsel prior to initiation.

H. SPECIAL ISSUES. In most cases, NRO use of the Internet is covered under the same laws, regulations, and procedures that govern computer fraud and misuse, unclassified telephone calls, and participation at professional conferences. These include regulations governing contacts with foreign nationals as well as contacts with the media and Congress. Users must also comply with the requirements and prohibitions of Executive Order 12333 which governs the collection, retention, and dissemination of information regarding U.S. persons and the operational use of U.S. persons. The Copyright Act, the Freedom of Information Act, the Privacy Act, and statutory federal records requirements also contain provisions with which NRO Internet users must comply. Users should consult the NRO Internet User Guidelines and the Office of General Counsel regarding any Internet activity that raises legal concerns.

/Signed/

Keith R. Hall
Director

OPR: CIO/COMM
NRO Security