

THIS FILE IS MADE AVAILABLE THROUGH THE DECLASSIFICATION EFFORTS AND RESEARCH OF:

# THE BLACK VAULT

THE BLACK VAULT IS THE LARGEST ONLINE FREEDOM OF INFORMATION ACT / GOVERNMENT RECORD CLEARING HOUSE IN THE WORLD. THE RESEARCH EFFORTS HERE ARE RESPONSIBLE FOR THE DECLASSIFICATION OF THOUSANDS OF DOCUMENTS THROUGHOUT THE U.S. GOVERNMENT, AND ALL CAN BE DOWNLOADED BY VISITING:

[HTTP://WWW.BLACKVAULT.COM](http://www.blackvault.com)

YOU ARE ENCOURAGED TO FORWARD THIS DOCUMENT TO YOUR FRIENDS, BUT PLEASE KEEP THIS IDENTIFYING IMAGE AT THE TOP OF THE .PDF SO OTHERS CAN DOWNLOAD MORE!



NATIONAL RECONNAISSANCE OFFICE

14675 Lee Road  
Chantilly, VA 20151-1715

14 August 2009

Mr. John R. Greenewald  
[REDACTED]

Dear Mr. Greenewald:

This is in response to your e-mail dated 29 May 2009, received in the Information Management Services Center of the National Reconnaissance Office (NRO) on 01 June 2009. Pursuant to the Freedom of Information Act (FOIA), you are requesting "copies of the following:

1. NROD 10-2
2. NROD 10-4
3. NROD 10-5
4. NROD 22-1
5. NROD 22-2
6. NROD 22-3
7. NROD 50-1
8. NROD 61-1
9. NROD 82-1a
10. NROD 110-2
11. NROD 120-1
12. NROD 120-2
13. NROD 120-3
14. NROD 120-4
15. NROD 120-5
16. NROD 121-1
17. NROI 150-4."

Your request has been processed in accordance with the FOIA, 5 U.S.C. § 552, as amended, and the NRO Operational File Exemption, 50 U.S.C. § 432a. A thorough search for records in our files and databases located seventeen records totaling sixty-four pages that are responsive to your request. As an interim release, on 23 June 2009, we provided to you fourteen previously-released records, consisting of fifty-four pages. These records were released to you in full. The remaining three

responsive records, consisting of ten pages, are being released to you in part.

Material withheld from release is denied pursuant to FOIA exemptions:

(b)(1) as properly classified information under Executive Order 12958, Sections 1.4(c) and 1.4(g); and exemption (b)(3) which applies to information specifically exempt by statute(s), specifically 50 U.S.C. § 403-1, which protects intelligence sources and methods from unauthorized disclosure, and 10 U.S.C. § 424 which states: "Except as required by the President or as provided in subsection (c), no provision of law shall be construed to require the disclosure of (1) The organization or any function . . . (2) . . . number of persons employed by or assigned or detailed to any such organization or the name, official title, occupational series, grade, or salary of any such person . . . (b) Covered Organizations . . . the National Reconnaissance Office"; and

(b)(2), which pertains solely to the internal rules and practices of an agency and allows the withholding of information which, if released, would allow circumvention of an organization rule, policy, or statute, thereby impeding the agency in the conduct of its mission.

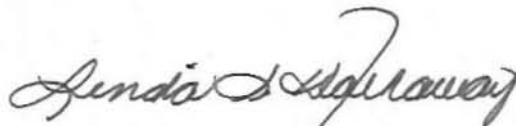
The FOIA authorizes federal agencies to assess fees for record services. Based upon the information provided, you have been placed in the "educational/scientific/media" category of requesters, which means you are responsible for duplication fees (.15 per page) exceeding 100 pages. Additional information about fees can be found on our website at [www.nro.gov](http://www.nro.gov).

In your request you expressed a willingness to pay fees up to the amount of \$10.00. In this case, no assessable fees were incurred.

You have the right to appeal this determination by addressing your appeal to the NRO Appeal Authority, 14675 Lee Road, Chantilly, VA 20151-1715, within 60 days of the above date. Should you decide to do this, please explain the basis of your appeal.

If you have any questions, please call the Requester Service Center at (703) 227-9326 and reference case number F09-0078.

Sincerely,

A handwritten signature in cursive script, reading "Linda S. Hathaway". The signature is written in dark ink and is positioned above the typed name.

Linda S. Hathaway  
Chief, Information Access  
and Release Team

enclosures: NROD 10-4, NROD 61-1, NROI 150-4



~~SECRET//BYE//SI//TK//X1~~

# National Reconnaissance Office

01 December 1999

NROD 10-4

Organization

---

**SUBJECT: National Reconnaissance Office Sensitive Activities Management Group**

---

**A. SYNOPSIS.** This Directive provides a structure to manage Sensitive Activities in the National Reconnaissance Office (NRO).

**B. AUTHORITY.** The NRO Sensitive Activities Management Group (SAMG) is created and this Directive is issued pursuant to the National Security Act of 1947, 50 U.S.C. §401 et seq., as amended; Executive Order 12333; Department of Defense Directive TS 5105.23, March 27, 1964, "National Reconnaissance Office"; and other applicable laws and directives.

**C. REFERENCES.** This Directive augments existing NRO Directives pertaining to: Organization, Audit and Oversight, Acquisition and Management and Operations.

**D. PURPOSE.** The NRO has engaged its mission partners and customers to improve integration of missions and special operational support requirements and activities. These partners and customers must address a dynamic and uncertain security environment. (b)(1)1.4g

(b)(1)1.4g To meet these varying and expanding requirements in a timely and responsive manner, the NRO must ensure that corporate management is postured to respond to these unique needs. While empowering action officers, this Directive establishes a senior NRO management structure to identify new security, policy or legal issues associated with NRO support to Sensitive Activities, and to assess whether there is a requirement for further review, approval, and/or congressional notification.

**E. SCOPE.** This Directive applies to all NRO Directorates, Offices and Staff Elements involved with supporting Sensitive Activities as defined below. This Directive does not replace, or substitute for, existing NRO policies and directives that support system development and acquisition efforts.

**NRO Approved For Release**

CL BY: (b)(3)  
CL REASON: 1.5(c)  
DECL ON: X1  
DRV FROM: NRO SCG 5.0  
01 October 1999

Handle via  
**BYEMAN/TALENT-KEYHOLE/COMINT**  
Channels Jointly

~~SECRET//BYE//SI//TK//X1~~

**F. DEFINITIONS.** For purposes of this Directive, Sensitive Activities shall be considered to include activities listed below, or as directed by the NRO Director or Deputy Director:

1. (b)(1)1.4c [REDACTED]  
(b)(1)1.4c [REDACTED]
2. (b)(1)1.4c [REDACTED]  
(b)(1)1.4c [REDACTED]
3. (b)(1)1.4c [REDACTED]
4. (b)(1)1.4c [REDACTED]
5. (b)(1)1.4c [REDACTED]  
(b)(1)1.4c [REDACTED]
6. Transfer of funds, personnel, equipment, property, or services between government agencies when related to support of Sensitive Activities.
7. (b)(1)1.4c [REDACTED]
8. Compartmented or special handling information operations.
9. (b)(1)1.4c [REDACTED]  
(b)(1)1.4c [REDACTED]

**G. RESPONSIBILITIES.**

1. To ensure that the NRO is prepared to respond in an efficient and timely manner when called on to support Sensitive Activities, this Directive establishes a SAMG. The SAMG will be the designated NRO entry point and approval authority for support to Sensitive Activities. The SAMG will also serve to ensure that appropriate legal and policy coordination is accomplished with mission partners, customers and users as needed. The Deputy Director for National Support (DDNS) will chair the SAMG.

2. The SAMG will be comprised of the DDNS, Deputy Director for Military Support, Director of Policy, Director Office of Security, and NRO General Counsel as legal advisor. The Deputy Director Resource Oversight and Management will be included in all discussions when the NRO may allocate resources to acquire or significantly modify an existing capability in support of a Sensitive Activity. On a case-by-case basis, the SAMG may include other Directors and key staff members as needed. The SAMG will provide appropriate corporate review and guidance to ensure NRO support is in accordance with applicable government policies and statutes.

**NRO Approved For Release**

Handle via  
BYEMAN/TALENT-KEYHOLE/COMINT  
Channels Jointly



**NROD 10-4  
Organization**

3. The SAMG administrative, staff, and executive secretary support will be provided by the Mission Integration Office (MIO). All requests for support to Sensitive Activities, identified above, will immediately be brought to the attention of Director MIO or the MIO representative designated as the SAMG Executive Secretary, who will notify the SAMG Chair and other members. A recommendation to convene the SAMG may be made by the SAMG Chair or by any SAMG member. Time-sensitive requests for support received outside of normal duty hours shall be directed to the

(b)(1)1.4c. (b)(2)High

(b)(3)

(b)(2) shall maintain a 24-hour capability to contact the Director MIO and other designated NRO Seniors.

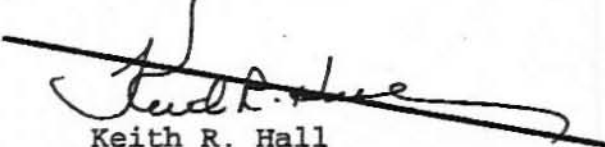
4. By their very nature, Sensitive Activities are not easily categorized. The full range of NRO capabilities may be needed to assist with activities brought to the SAMG. This Directive is not intended to circumvent established day-to-day organizational and procedural relationships with customers and mission partners nor interfere with, or substitute for, the normal conduct of day-to-day activities. Rather, the SAMG will consider activities that have unique time-sensitive and security-sensitive constraints as well as provide a responsive decision-making forum to address those activities not covered by existing NRO legal or operational policies. On a by-exception basis, Sensitive Activity decisions having potential community-wide implications will be forwarded to the Director NRO or Deputy Director NRO for coordination.

5. Any incidents associated with, or resulting from, NRO support to Sensitive Activities shall be reported immediately to the SAMG.

**H. APPROVAL.**

1. The DDNS will issue and retain Memorandums for Record (MFRs) for all recommendations and decisions of the SAMG; these MFRs will be routed through the DNRO.

2. General guidance pertaining to waivers and applicability of this Directive will be established and disseminated by the SAMG and maintained by the DDNS.

  
Keith R. Hall  
Director

OPR: National Support Staff

**NRO Approved For Release**

Handle via  
BYEMAN/TALENT-KEYHOLE/COMINT  
Channels Jointly



~~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

**NRO Approved For Release**

~~SECRET~~



~~SECRET~~

NROD 61-1  
Information Technology

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

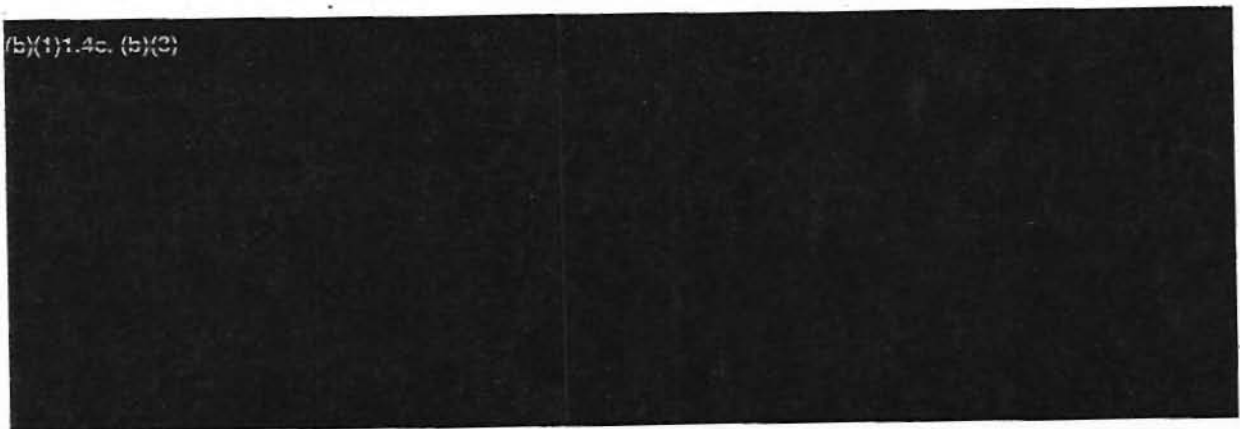
3. The NRO acknowledges the risk of attack against its Internet systems and the potential for inadvertent or unauthorized release of classified information on the Internet. It has deployed and will continue to employ protective mechanisms against external attacks. The NRO relies on each user's compliance 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)1.4c, (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)1.4c, (b)(2)



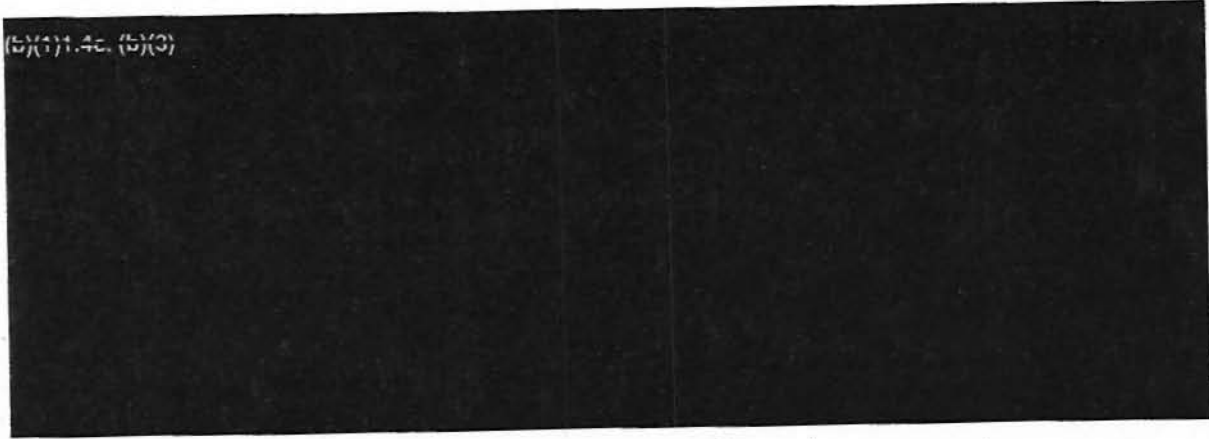
~~SECRET~~

NRO Approved For Release

~~SECRET~~

NROD 61-1  
Information Technology

(S)(1)1.4c. (S)(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).

~~SECRET~~

NRO Approved For Release

~~SECRET~~

NROD 61-1  
Information Technology

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.

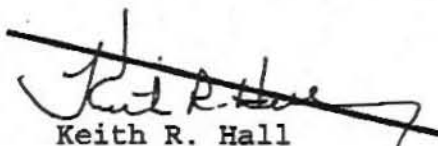
NRO Approved For Release

4  
**SECRET**

**SECRET**

**NROD 61-1**  
**Information Technology**

**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.

  
Keith R. Hall  
Director

OPR: CIO/COMM  
NRO Security

**NRO Approved For Release**

~~**SECRET**~~



~~FOR OFFICIAL USE ONLY~~

# National Reconnaissance Office

6 January 1998

NROI 150-4

Facilities Management

---

**SUBJECT: Prohibited Items in NRO Headquarters Buildings/Property**

---

**A. SYNOPSIS.** This instruction identifies items that are prohibited in National Reconnaissance Office (NRO) Headquarters (HQS) buildings and/or property. Individuals in violation of these prohibitions may be subject to administrative sanctions and/or criminal prosecution.

**B. AUTHORITY.**

1. 18 U.S.C. § 930
2. 32 CFR 1903.7; 1903.10
3. NRO Security Manual (BSM, dated June 1993)
4. DCID 1/21, Annex D, Part I
5. NRO Policy Directive 002/95

**C. PURPOSE.** The purpose of this instruction is to identify items that are prohibited in NRO HQS buildings and/or property.

**D. DEFINITIONS.**

1. **Dangerous Weapons:** Firearms, ammunition, explosives, incendiary devices, blades, knives (other than small pocket-knives), and any other instrument or material that is used for, or is readily capable of, causing death or serious bodily injury.

2. **Illegal Substances:** Any item that is identified by federal or state statute as unlawful to possess without appropriate authorization (e.g., illegal narcotics, nuclear materials, biological or chemical agents).

3. **NRO HQS:** Westfields, (b)(3)  
(b)(3) for the purposes of this instruction.

4. **Non-Approved Electronic Equipment:** Personally owned cellular phones, laptops, and associated media;

**NRO Approved For Release**

~~FOR OFFICIAL USE ONLY~~



NROI 150-4  
Facilities Management

and recording devices. (For more specific guidance, see NRO Policy Directive 002/95 and DCID 1/21, Annex D, Part I, located on the Office of Security Homepage on the NRO "Bye-way.")

**E. PROHIBITED ITEMS.**

1. The following items are not permitted on NRO HQS property unless expressly permitted for official reasons:

- a) Dangerous Weapons
- b) Illegal Substances
- c) Animals other than Guide Dogs

2. In addition to the items listed in E.1, the following items are not permitted in NRO HQS buildings, nor may they be used on NRO HQS property, unless expressly permitted for official reasons:

- a) Cameras and Photographic Equipment
- b) Alcoholic Beverages
- c) Non-approved Electronic Equipment

**F. EXCEPTIONS.** Requests for all exceptions, excluding alcohol, will be addressed on a case-by-case basis by contacting the Facility Duty Officer at 850-6161. Directorate and Office heads may approve the introduction of alcohol into NRO HQS buildings on special occasions.

**G. QUESTIONS.** Questions pertaining to this instruction may be directed to Management Services & Operations/Headquarters Security Services Group at secure 850-5048 or 850-5200.

  
Roger C. Marsh

Director, Management  
Services and Operations

OPR: MS&O/HSSG

**NRO Approved For Release**