

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

11 July 2007

2007-4217

**MEMORANDUM OF UNDERSTANDING  
BETWEEN  
THE NATIONAL RECONNAISSANCE OFFICE,  
CHIEF INFORMATION OFFICER  
AND  
THE DEPARTMENT OF HOMELAND SECURITY,  
OFFICE OF INTELLIGENCE AND ANALYSIS,  
CHIEF INFORMATION OFFICER  
ON  
THE USE OF DEPARTMENT OF HOMELAND SECURITY WORKSTATIONS TO  
CONNECT TO THE NATIONAL RECONNAISSANCE OFFICE  
MANAGEMENT INFORMATION SYSTEM**

- A. (~~U//FOUO~~) PURPOSE.** This Memorandum of Understanding (MOU) formally documents the information assurance responsibilities between the National Reconnaissance Office (NRO) and the Department of Homeland Security (DHS) for providing Sensitive Compartmented Information (SCI) electronic access to the NRO Management Information System (NMIS) for NRO liaison personnel stationed at DHS.
- B. (~~U//FOUO~~) REFERENCES.**
1. (U) Director of Central Intelligence Directive (DCID) 6/3, Protecting Sensitive Compartmented Information Within Information Systems, 5 June 1999
  2. (U) DCID 6/9, Physical Security Standards for Sensitive Compartmented Facilities, 18 November 2002
  3. (U) NRO Instruction 60-1a, Approval Procedures for Information Technology Services Provided by the Communications Systems Acquisition and Operations Directorate, 30 November 2001
- C. (~~U//FOUO~~) BACKGROUND.** Connectivity from DHS to NRO provides NRO personnel assigned and deployed to DHS the capability to access the NMIS from an SCI DHS workstation. This capability leverages existing SCI network connectivity with minimal additional resource requirements while allowing NRO personnel the necessary access to perform their duties.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

SUBJECT: (U//~~FOUO~~) MOU BETWEEN THE NRO, CIO AND DHS, OFFICE OF INTELLIGENCE AND ANALYSIS, CIO ON THE USE OF NMIS

D. (U) RESPONSIBILITIES.

1. (U//~~FOUO~~) NRO will:

a. (U//~~FOUO~~) Maintain configuration control over NRO communications systems and equipment and coordinate any changes that may affect external interfaces.

b. (U//~~FOUO~~) Validate eligibility; track, monitor, and rescind user access as required.

c. (U//~~FOUO~~) Provide all applicable initial and refresher security and information assurance training to NRO personnel.

d. (U//~~FOUO~~) Brief NRO users of their responsibility to comply with NRO and applicable DHS information security policy and procedures.

e. (U//~~FOUO~~) Report all information technology (IT) and information assurance incidents for all NRO users to appropriate entities such as the Intelligence Community-Incident Response Center.

f. (U//~~FOUO~~) Provide helpdesk support to NRO users accessing NMIS.

g. (U//~~FOUO~~) Ensure NRO users meet all of the following criteria and forward this information to the appropriate DHS security point of contact as required:

(1) (U//~~FOUO~~) Hold United States (U.S.) citizenship.

(2) (U//~~FOUO~~) Provide support to the NRO as a U.S. Government employee, NRO-sponsored contractor, or NRO Federally Funded Research and Development Center employee.

(3) (U//~~FOUO~~) Hold a current Top Secret clearance and be indoctrinated for the appropriate SCI.

(4) (U//~~FOUO~~) Be subject to or have a counter-intelligence scope security polygraph that has

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

SUBJECT: (U//~~FOUO~~) MOU BETWEEN THE NRO, CIO AND DHS, OFFICE OF INTELLIGENCE AND ANALYSIS, CIO ON THE USE OF NMIS

been favorably adjudicated and is accepted by the NRO.

(5) (U//~~FOUO~~) Have a need-to-know for information on NMIS that is validated by an NRO Government sponsor.

2. (U//~~FOUO~~) DHS will:

a. (U//~~FOUO~~) Ensure systems that will access NMIS are certified and accredited according to Reference B. 1.

b. (U//~~FOUO~~) Ensure the NRO user is properly indoctrinated for all relevant SCI compartments prior to creating a local account.

c. (U//~~FOUO~~) Notify the NRO Director of Security and Counterintelligence immediately of any reportable IT security incidents, user access terminations, and security concerns affecting NRO personnel at DHS who have access to NMIS.

d. (U//~~FOUO~~) Provide, upon request by NRO Chief Information Officer (CIO), audit records of users' local sessions on DHS workstations to include username, session initiation date and time, workstation Internet Protocol address, and session termination date and time.

e. (U//~~FOUO~~) Provide training to deployed NRO users regarding their security responsibilities for using a DHS workstation within a DHS sensitive compartment information facility.

**E. (U) IMPLEMENTATION.**

1. (U) This MOU will take effect upon signature of authorized representatives from the NRO CIO and DHS Intelligence and Analysis CIO.

2. (U) As agreed to by all parties, or designees, this MOU shall be reviewed every two years to determine its continued applicability.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

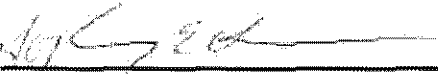
~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

SUBJECT: (U//~~FOUO~~) MOU BETWEEN THE NRO, CIO AND DHS, OFFICE OF INTELLIGENCE AND ANALYSIS, CIO ON THE USE OF NMIS

3. (U) Either party may terminate this MOU by written notification to the other party 180 days in advance of the termination date. This MOU will terminate after such written notification.

Craig Kaucher  
Chief Information Officer  
Office of Intelligence and  
Analysis  
Department of Homeland Security

Dr. Susan Gragg  
Chief Information Officer  
National Reconnaissance Office

7/24/07   
Date

7/12/2007   
Date

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~