(b)(1) [redacted]

NORTH AMERICAN AEROSPACE DEFENSE COMMAND
AND
UNITED STATES NORTHERN COMMAND

MEMORANDUM FOR DIRECTOR OF OPERATIONS,
JOINT STAFF

SEP 0 3 2010

FROM: Commander, NORAD and USNORTHCOM
250 Vandenberg Street, Suite B016
Peterson AFB CO 80914-3801

SUBJECT: (U//~~FOUO)~~ NORAD and USNORTHCOM Response to WikiLeaks PLANORD

1. (U//~~FOUO)~~ Thank you for the opportunity to provide our inputs on the serious situation concerning WikiLeaks. We are extremely sensitive to the risks to our missions and personnel if classified information gets to our adversaries via unclassified, unrestricted, and open source media.

2. (U//~~FOUO)~~ We have reviewed and assessed our operations and protection measures and are confident that NORAD and USNORTHCOM are in compliance with all applicable directives to protect classified information. We are also taking steps to increase protection measures across both commands.

3. (U) NORAD and USNORTHCOM stand ready to answer any further questions on this matter. Our POC is (b)(6) [redacted] LTC, USA, Director, Command Security. He can be reached at (719) 556-5662 or by email at (b)(6) [redacted] @northcom.mil or (b)(6) [redacted] @northcom.smil.mil.

JAMES A. WINNEFELD, Jr.
Admiral, USN

Attachment:
(U) NORAD and USNORTHCOM Response ((b)(1) [redacted]

(b)(1) [redacted]

This Memorandum is Unclassified // ~~For Official Use Only~~ When Attachment is Removed

NORTH AMERICAN AEROSPACE DEFENSE COMMAND
AND
UNITED STATES NORTHERN COMMAND

(U//~~FOUO~~) NORAD and USNORTHCOM Response to WikiLeaks PLANORD

3A. (b)(1)
(b)(1)

(U) On 11 August 2010, SecDef directed an investigation due to the WikiLeaks incident. This led to a PLANORD directing Combatant Commands and Services to review the impact of unauthorized release of classified information and to answer 15 related questions. The HQ NORAD and USNORTHCOM Insider Threat Working Group (ITWG) met on 16 and 17 August 2010 to address the following tasks.

3.B.2.A. (b)(1)
(b)(1)

(b)(1)
(b)(1)

(b)(1)
(b)(1)

(b)(1)
(b)(1)

Derived from: CJCS Message dated 121451Z Aug 10
Subj: WikiLeaks Planord, USMC: DJ-3
Declassify on: 121352Z Aug 2035

Mr. (b)(6)
NORAD and USNORTHCOM
Chief, Collateral Security

(b)(1) (b)(1) [redacted]

(b)(1) (b)(1) [redacted]

(b)(1) (b)(1) [redacted]

3.B.2.C. (b)(1) (b)(1) [redacted]

(b)(1) (b)(1) [redacted]

(b)(1) (b)(1) [redacted]

(b)(1) (b)(1) [redacted]

(b)(1) (b)(1) [redacted]

3.B.2.D. (b)(1) (b)(1) [redacted]

(b)(1) (b)(1) [redacted]

(b)(1) (b)(1) [redacted]

(b)(1)
(b)(1)

3.B.2.E. (b)(1)
(b)(1)

(b)(1)
(b)(1)

(b)(1)
(b)(1)

3.B.2.F. (b)(1)
(b)(1)

(b)(1)
(b)(1)

(U) Individuals with an interim secret clearance are required to comply with a strict prescreen process which both the security manager and commander review prior to granting access to classified information or programs. There are no other restrictive measures placed on a person granted an interim security clearance. If an incident warrants review, a clearance requires removal, or the final Central Adjudication Facility adjudication results in disapproval, the member's access is immediately removed.

3.B.2.G. (b)(1) (b)(1) [redacted]

(b)(1) [redacted]

(U) IAW AFMAN 14-304, the Command Security Directorate reports administrative changes for clearance status information of individuals with collateral security clearances. For personnel cleared for collateral Secret and/or Top Secret clearance, derogatory information generates a Security Information File (SIF). A SIF is a collection of documents generated because of the discovery or development of unfavorable information, which brings into question a person's continuing eligibility for a security clearance or access to SCI. A commander, civilian equivalent or the Central Adjudication Facility initiates a SIF. The SIF serves as a repository for unfavorable or derogatory information that requires further review, evaluation, or investigation to resolve outstanding administrative or adjudicative concerns.

3.B.2.H. (b)(1) (b)(1) [redacted]

(b)(1) (b)(1) [redacted]

(b)(1) (b)(1) [redacted]

(b)(1) (b)(1) [redacted]

3.B.2.I. (b)(1) (b)(1) [redacted]

(b)(1) (b)(1) [redacted]

(b)(1) [redacted]

3.B.2.J. (b)(1) (b)(1) [redacted]

(b)(1) (b)(1) [redacted]

3.B.2.K. (b)(1) (b)(1) [redacted]

(b)(1) (b)(1) [redacted]

(U) J25S (SSO) POC is (b)(6) [redacted] DSN: 692-3343.
(U) OPSEC POC is Maj (b)(6) [redacted] DSN: 834-0664.
(U) Command Security POC is (b)(6) [redacted], DSN: 834-2158.

3.B.2.L. (b)(1) [redacted]

(U) Security incidents involving collateral classified are processed IAW EO 13526, DOD 5200.1R DOD *Information Security Program* and AFI 31-401 *Information Security Program.* A cyber-domain incident requires the command Network Operations Security Center (NOSC) to take immediate actions to prevent further compromise. All notifications to include any far-end users' systems administrators ensure further spread of classified information. An impartial investigating officer investigates all security incidents that potentially compromise security information. The Judge Advocate and the 21SW review all investigations, and the N/NC Chief of Staff direct final action based on recommendations from the Command Security Director. The Command Security Director provides the Deputy Chief of Staff with security incident data to ensure top-down situational awareness and emphasis.

(b)(1) (b)(1) [redacted]

(U) IAW Joint Air Force Army Navy (JFAN) 6/0 as the primary directive and DOD 5200.1R DOD *Information Security Program*, Special Access Program (SAP) security violations/infractions require reporting within 24 hrs of discovery to the affected Program Security Office (PSO) and the chain of command. The PSO through the chain of command must promptly advise the service component Special Access Program Control Office (SAPCO) in all instances where national security concerns would affect collateral security programs or clearances of program-accessed individuals. The PSO reports violations to the government program manager with additional notification to the service component SAPCO. All security violations or infractions require a preliminary investigation. The seriousness of damage to U.S. interests must be determined and appropriate measures taken to negate or minimize the adverse effect of any potential compromise. In all cases, the Command takes appropriate action to identify the source and reason for the actual or potential compromise.

3.B.2.M. (b)(1)
(b)(1)

(b)(1)
(b)(1)

(b)(1)
(b)(1)

3.B.2.N. (b)(1)
(b)(1)

(b)(1)
(b)(1)

3.B.2.O. (b)(1)
(b)(1)

(b)(1)
(b)(1)

CLASSIFICATION: (b) (1) ([redacted])

DISSEMINATION CONTROL: (b) (1) ([redacted])

NORAD and USNORTHCOM Staff Summary Sheet (SSS), 23 JUN 10

Date: *20 Aug 2010*

//APPROVAL/ROUTING//

TO:	**ACTION:**	**LAST NAME, RANK, and DATE**	
N-NC/J1	COORD	(b) (6) ([redacted])Col	17 Aug 10
N-NC/J2	COORD	(b) (6) ([redacted] ,) CAPT	16 Aug 10
N/J3	COORD	(b) (6) ([redacted])for Gen Forgues	17 Aug 10
NC/J3	COORD	(b) (6) ([redacted])Col	17 Aug 10
N-NC/J4	COORD	(b) (6) ([redacted])for BG Harrell	17 Aug 10
N-NC/J5	COORD	(b) (6) ([redacted] ,)Col	18 Aug 10
N-NC/J6	COORD	[redacted])CAPT	18 Aug 10
N-NC/J7	COORD	Mr. Pino, SES	16 Aug 10
N-NC/J8	COORD	Mr. Carpenter, SES	18 Aug 10
N-NC/IC	COORD	(b) (6) (Mr. [redacted])Civ	16 Aug 10
NC/SJFHQ	COORD	(b) (6) ([redacted])Col	16 Aug 10
N-NC/CP	COORD	Ms. (b) (6) ([redacted])Civ	13 Aug 10
N-NC/CSC	COORD	Mr. (b) (6) ([redacted])Civ	13 Aug 10
N-NC/HC	COORD	[redacted])Col	16 Aug 10
N-NC/HO	COORD	Mr. (b) (6) ([redacted] ,)Civ	16 Aug 10
N-NC/IG	COORD	(b) (6) ([redacted])Col	18 Aug 10
N-NC/JA	COORD	(b) (6) ([redacted])Civ	20 Aug 10
N-NC/NG	COORD	(b) (6) ([redacted])Col	16 Aug 10
N-NC/PA	COORD	(b) (6) ([redacted])Civ	13 Aug 10
N-NC/RF	COORD	(b) (6) ([redacted])Col	17 Aug 10
N-NC/SG	COORD	(b) (6) ([redacted])Col	16 Aug 10
N-NC/WO	COORD	(b) (6) ([redacted])Civ	18 Aug 10
CANPOLAD	COORD	No Response	
USPOLAD	COORD	(b) (6) ([redacted]) for Mr. [redacted], DV6	16 Aug 10
N-NC/LA	COORD	Ms. (b) (6) ([redacted])Civ	17 Aug 10
N-NC/CSEL	COORD	(b) (6) ([redacted])SMSgt	17 Aug 10
N-NC/CX	COORD	(b) (6) ([redacted])Col	13 Aug 10
SJS	COORD		
CS	COORD		
DC	INFO	Copy Provided	
ND	COORD		
CDR	SIGN		

ACTION OFFICER: (U) GS-12, (b) (6) ([redacted]) USAF Civilian, N-NC/CSO, DSN 834-2158.
(U) GS-12, (b) (6) ([redacted]) DIA Civilian, N-NC/SSO, DSN 692-3888.

SUSPENSE: (U) CJCS/J39, 2 Sep 10 in response to WikiLeaks Planord

CLASSIFICATION (b)(1)[redacted]

CLASSIFICATION: (b) (1) ([redacted])

DISSEMINATION CONTROL: (b) (1) ([redacted])
SUBJECT: (U//~~FOUO~~) 4 Star - PLANORD and SecDef Memorandums regarding WikiLeaks

PURPOSE: (U//~~FOUO~~) Request the Commander approve and sign the attached Memorandum at (Tab 1) concerning NORAD and USNORTHCOMs response to Wikileaks PLANORD issued by CJCS.

BOTTOM LINE: (U//~~FOUO~~) On 11 August SECDEF directed an investigation (Tab 2) as a result of the WikiLeaks incident. This led to a WIKILEAKS PLANORD (Tab 3) being released which directed Combatant Commands and Services to review impact of unauthorized release of classified information and to answer 15 related questions.

BACKGROUND: (U//~~FOUO~~) PLANORD directs Combatant Commands and Services to conduct planning and research on described tasks to outline the effect of the Wikilieaks incident on each command. Command Security Office (CSO) is the Command Lead for this effort.

DISCUSSION: (b) (1) ([redacted])

RECOMMENDATION: (U//~~FOUO~~) Request the Commander approve and sign the attached Memorandum at (Tab 1) to provide NORAD and USNORTHCOMs response to Wikileaks PLANORD issued by CJCS. Our external suspense to CJCS is 2 Sep 2010.

APPROVED/SIGNED: (b) (6) ([redacted],) LTC, USA – Director, Command Security

3 TABS:
1. (b) (6) ([redacted])
2. (U//~~FOUO~~) SECDEF Memorandums
3. (b) (1) ([redacted])

Derived from: CJCS Message dated 121451Z Aug 10
Subj: WikiLeaks Planord, USMC: DJ-3
Declassify on: 121352Z Aug 2035

Mr. (b) (6) ([redacted])
NORAD and USNORTHCOM
Chief, Collateral Security

CLASSIFICATION (b)(1)[redacted]

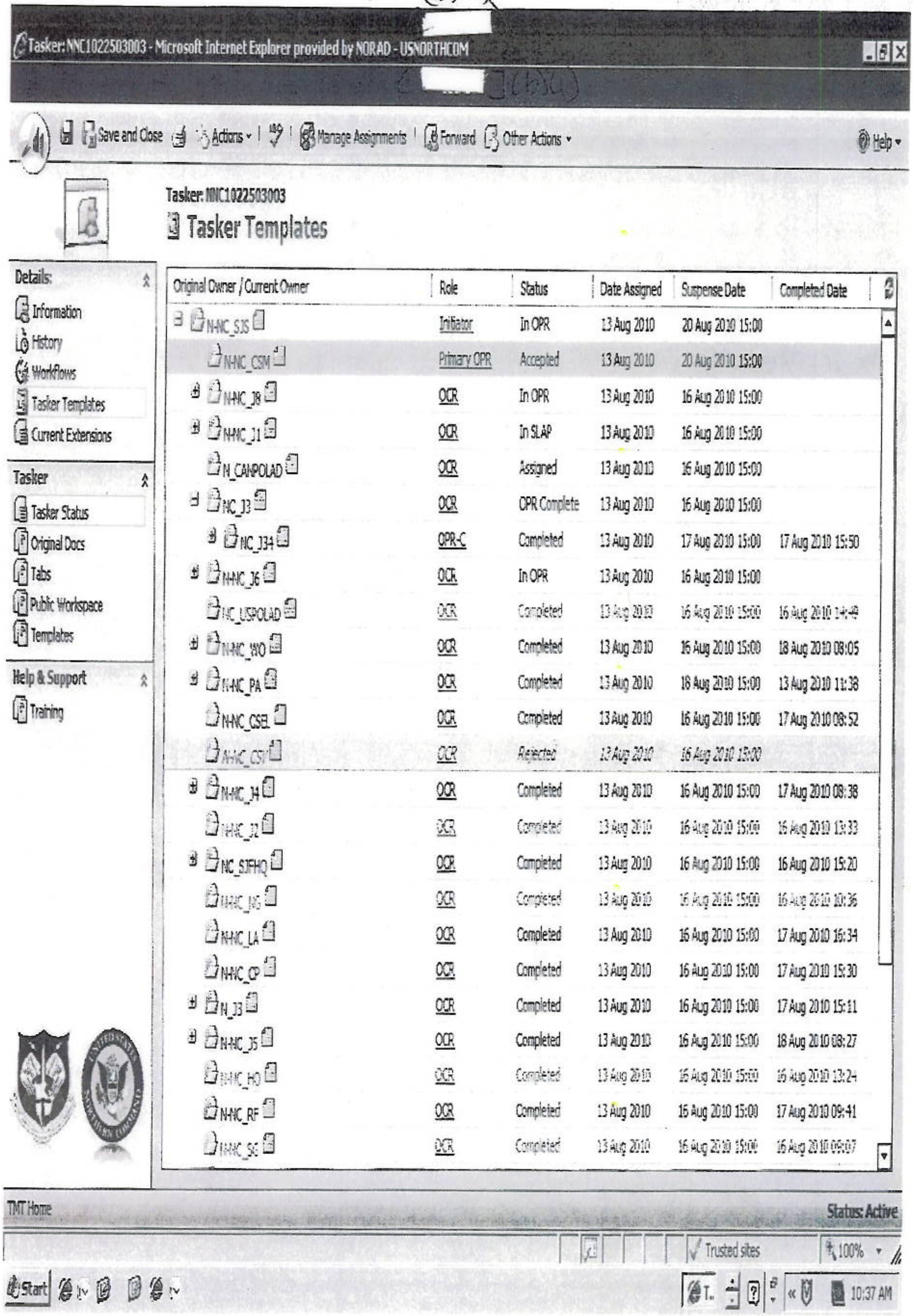
	RESPONSE
(b)(1) [redacted]	J2: In March 2010 HQ NORAD and USNORTHCOM started an Insider Threat Working Group. Currently the ITWG Charter is in development and key sub groups are being identified. N-NC/J39 Cyber Operations Team: Provided list of known extrimist web-sites and "dirty-works" to Cyber Fusion Cell Lead, LT Co (b)(6) [redacted] for implamentation on the N-NC NIPR and notified N-NC ITWG of efforts.
(b)(1) [redacted]	J2: Insider Threat training is addressed during N-NC 101 (CI Awareness Training). This training is mandatory for all newly assigned personnel, and annually via the LMS module. CISE is working with JCITA to load module onto N-NC LMS system as an emphasis program for all newcomers.
(b)(1) [redacted]	J2: Cybercom has developed a plan to block this website and is waiting on approval to proceed. Blocking WikiLeaks does not mitigate all risk. The level of risk to the N-NC is minimal. N-NC/J39 Cyber Operations Team: N/A for the first part, for the second part; operational impact can not be evaluated until we know and can evaluate documents that where downloaded to our NIPR from WikiLeaks.
(b)(1) [redacted]	J6: HBSS, J2: Scanners and digital senders also pose risk.
Describe IA controls applied to restrict access to information based on need-to-know.	J2: Requests for JWICS accounts have to be justified by a supervisor and approved by the SSO. The SSO reviews account requests for proper need-to-know. PKI, portal restrictions, security groups.

Describe any additonal administrative or technical oversight places on individuals with an interim secret clearance in order to monitor/manage access to classified information.	Command Security: (U) Individuals with an interim secret clearance are required to comply with a strict prescreen process in which the security manager and commander review prior to granting access to classified information or programs. There are no other restrictive measures placed on a member granted an Interim security clearance. If the adjudication comes back with disapproval the member has access immediately removed.
(b)(6) [redacted]	J2: Derogatory information on an individual is reported through either self, employee/supervisor, or LE/CI development Once information is reported, it is either investigated by the command through the Command Directed Inquiry (CDI), or through an investigation lead by AFOSI (Executive Agency). Results of the inquiry/investigation are provided to element commander of the affected service, Special Security Officer and N-NC Commander. Element Commander takes UCMJ action, if appropriate. If no UCMJ action is taken, SSO compiles recommendations for individuals supervisor/leadership, SSO along with inquiry/investigation results and is forwarded to the service adjudication authority for clearance/access determination.
(b)(1) [redacted]	J2: Insider Threat Working Group is under development.
(b)(1) [redacted]	J2: To access classified N-NC personnel must have a valid security clearance required for that classification. To transport SCI N-NC must complete courier training and have a valid courier badge.
(b)(1) [redacted]	N-NC/J39 Cyber Operations Team: CD/DVD burning in J39 is controlled by our SASM. If unable to burn CDs/DVDs we will be unable to utilize the STO conference room for S//NOFORN briefs created on the SIPRnet.

(b)(1)	J2: The development of the Insider Threat Working Group is underway at N-NC. Currently, OPSEC, CI and Security disciplines are represented at the Insider Threat Working Group. A new charter is being developed to address who has the lead on a specific pillar, as outlined in the Insider Threat Implementation Plan The Charter will also address how the information is shared within the ITWG.
(b)(1)	(U) Security incidents are processed IAW EO 13526, DOD 5200.1R DOD Information Security Program and AFI 31-401: Security incidents are reported to individual chain of command, then directorate Security Manager, in-turn notifies Command Security, who in-turn notifies Installation 21st SW Information Security office. Immediate notifications are made depending on the incident; cyber domain involves our computer systems Help Desk and NOSC - take all actions to segregate and isolate to prevent futher compromise, all notifications are made to personnel involved to prevent further spread. Impartial Inquiry officer is assigned to the case to throughly investigate the incident. Reports are reviewed by Command Security, Judge Advocate, 21SW, and final actions are taken based on the report by the NNC Chief of Staff, and offenders individual Director to prevent future incidents. The Command Security Office provides the Deputy Chief of Staff with data with top-down emphasis to prevent incidents within the command.
Describe your procedures for auditing the usage of information systems and reviewing the results.	
Describe any challenges you are experiening in complying with the DISA security technical implementation guides. Provide details as necessary.	
Describe any unique requirements and challenges in executing your security program.	J2: Bi-National Command.

(b)(1)

[redacted]



Tasker: NNC1022503003 - Microsoft Internet Explorer provided by NORAD - USNORTHCOM

[redacted] (b)(1)

Tasker: NNC1022503003

Tasker Templates

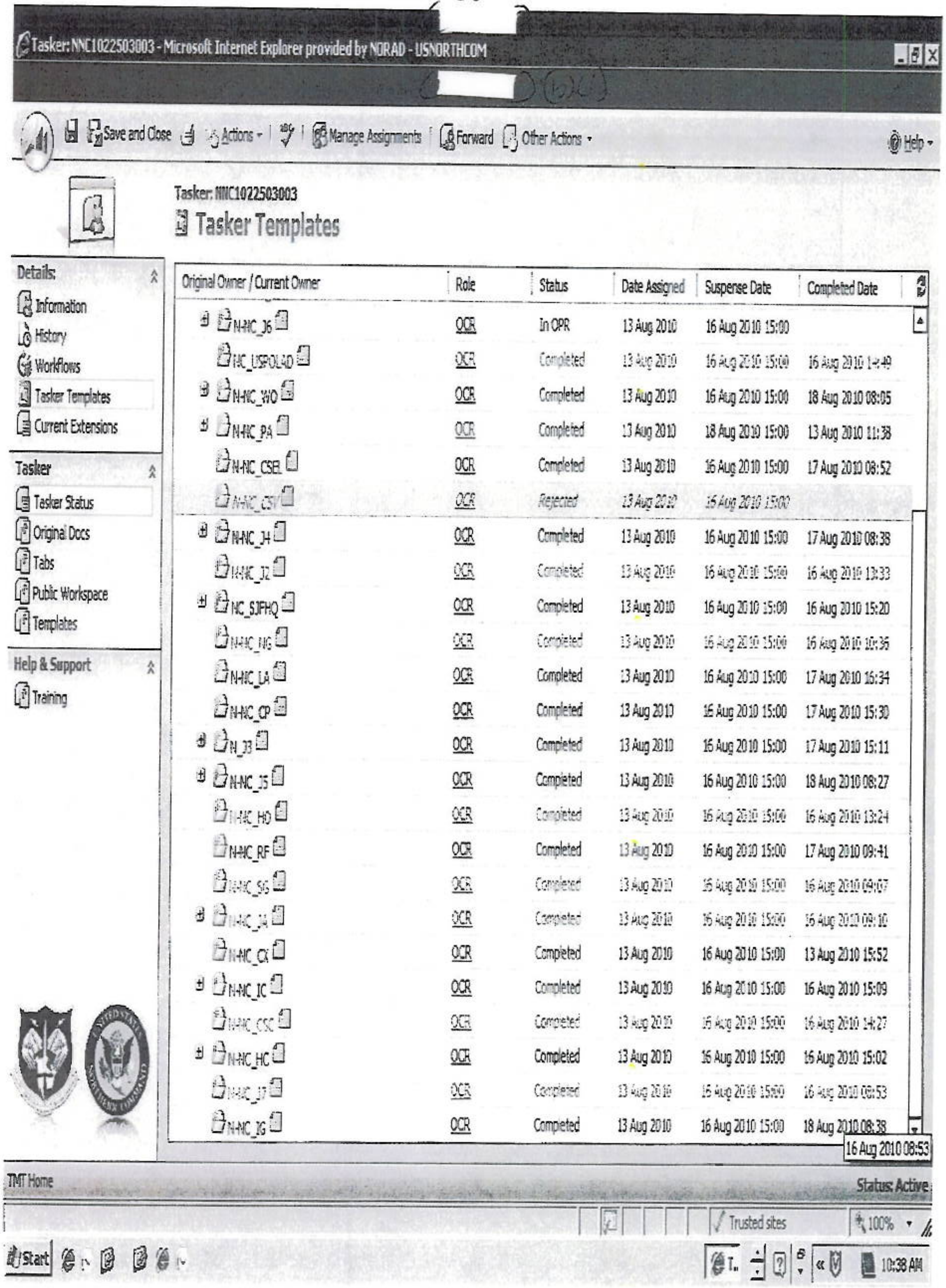
Original Owner / Current Owner	Role	Status	Date Assigned	Suspense Date	Completed Date
N-NC_SJS	Initiator	In OPR	13 Aug 2010	20 Aug 2010 15:00	
N-NC_CSM	Primary OPR	Accepted	13 Aug 2010	20 Aug 2010 15:00	
N-NC_J8	OCR	In OPR	13 Aug 2010	16 Aug 2010 15:00	
N-NC_J1	OCR	In SLAP	13 Aug 2010	16 Aug 2010 15:00	
N_CANPOLAD	OCR	Assigned	13 Aug 2010	16 Aug 2010 15:00	
NC_J3	OCR	OPR Complete	13 Aug 2010	16 Aug 2010 15:00	
NC_J34	OPR-C	Completed	13 Aug 2010	17 Aug 2010 15:00	17 Aug 2010 15:50
N-NC_J6	OCR	In OPR	13 Aug 2010	16 Aug 2010 15:00	
NC_USPOLAD	OCR	Completed	13 Aug 2010	16 Aug 2010 15:00	16 Aug 2010 14:49
N-NC_WO	OCR	Completed	13 Aug 2010	16 Aug 2010 15:00	18 Aug 2010 08:05
N-NC_PA	OCR	Completed	13 Aug 2010	18 Aug 2010 15:00	13 Aug 2010 11:38
N-NC_CSEL	OCR	Completed	13 Aug 2010	16 Aug 2010 15:00	17 Aug 2010 08:52
N-NC_CSI	OCR	Rejected	13 Aug 2010	16 Aug 2010 15:00	
N-NC_J4	OCR	Completed	13 Aug 2010	16 Aug 2010 15:00	17 Aug 2010 08:38
N-NC_J2	OCR	Completed	13 Aug 2010	16 Aug 2010 15:00	16 Aug 2010 13:33
NC_SJFHQ	OCR	Completed	13 Aug 2010	16 Aug 2010 15:00	16 Aug 2010 15:20
N-NC_NG	OCR	Completed	13 Aug 2010	16 Aug 2010 15:00	16 Aug 2010 10:36
N-NC_LA	OCR	Completed	13 Aug 2010	16 Aug 2010 15:00	17 Aug 2010 16:34
N-NC_CP	OCR	Completed	13 Aug 2010	16 Aug 2010 15:00	17 Aug 2010 15:30
N_J3	OCR	Completed	13 Aug 2010	16 Aug 2010 15:00	17 Aug 2010 15:11
N-NC_J5	OCR	Completed	13 Aug 2010	16 Aug 2010 15:00	18 Aug 2010 08:27
N-NC_HO	OCR	Completed	13 Aug 2010	16 Aug 2010 15:00	16 Aug 2010 13:24
N-NC_RF	OCR	Completed	13 Aug 2010	16 Aug 2010 15:00	17 Aug 2010 09:41
N-NC_SG	OCR	Completed	13 Aug 2010	16 Aug 2010 15:00	16 Aug 2010 09:07

TMT Home

Status: Active

(b)(1)

[redacted]



Tasker: NNC1022503003 - Microsoft Internet Explorer provided by NORAD - USNORTHCOM

[redacted] (b)(1)

Tasker: NNC1022503003

Tasker Templates

Original Owner / Current Owner	Role	Status	Date Assigned	Suspense Date	Completed Date
N-NC_J6	OCR	In OPR	13 Aug 2010	16 Aug 2010 15:00	
NC_USPOLAD	OCR	Completed	13 Aug 2010	16 Aug 2010 15:00	16 Aug 2010 14:49
N-NC_WO	OCR	Completed	13 Aug 2010	16 Aug 2010 15:00	18 Aug 2010 08:05
N-NC_PA	OCR	Completed	13 Aug 2010	18 Aug 2010 15:00	13 Aug 2010 11:38
N-NC_CSEL	OCR	Completed	13 Aug 2010	16 Aug 2010 15:00	17 Aug 2010 08:52
N-NC_CSV	OCR	Rejected	13 Aug 2010	16 Aug 2010 15:00	
N-NC_J4	OCR	Completed	13 Aug 2010	16 Aug 2010 15:00	17 Aug 2010 08:38
N-NC_J2	OCR	Completed	13 Aug 2010	16 Aug 2010 15:00	16 Aug 2010 13:33
NC_SJFHQ	OCR	Completed	13 Aug 2010	16 Aug 2010 15:00	16 Aug 2010 15:20
N-NC_NG	OCR	Completed	13 Aug 2010	16 Aug 2010 15:00	16 Aug 2010 10:36
N-NC_LA	OCR	Completed	13 Aug 2010	16 Aug 2010 15:00	17 Aug 2010 16:34
N-NC_CP	OCR	Completed	13 Aug 2010	16 Aug 2010 15:00	17 Aug 2010 15:30
N_J3	OCR	Completed	13 Aug 2010	16 Aug 2010 15:00	17 Aug 2010 15:11
N-NC_J5	OCR	Completed	13 Aug 2010	16 Aug 2010 15:00	18 Aug 2010 08:27
N-NC_HO	OCR	Completed	13 Aug 2010	16 Aug 2010 15:00	16 Aug 2010 13:24
N-NC_RF	OCR	Completed	13 Aug 2010	16 Aug 2010 15:00	17 Aug 2010 09:41
N-NC_SG	OCR	Completed	13 Aug 2010	16 Aug 2010 15:00	16 Aug 2010 09:07
N-NC_J4	OCR	Completed	13 Aug 2010	16 Aug 2010 15:00	16 Aug 2010 09:10
N-NC_CX	OCR	Completed	13 Aug 2010	16 Aug 2010 15:00	13 Aug 2010 15:52
N-NC_IC	OCR	Completed	13 Aug 2010	16 Aug 2010 15:00	16 Aug 2010 15:09
N-NC_CSC	OCR	Completed	13 Aug 2010	16 Aug 2010 15:00	16 Aug 2010 14:27
N-NC_HC	OCR	Completed	13 Aug 2010	16 Aug 2010 15:00	16 Aug 2010 15:02
N-NC_J7	OCR	Completed	13 Aug 2010	16 Aug 2010 15:00	16 Aug 2010 08:53
N-NC_IG	OCR	Completed	13 Aug 2010	16 Aug 2010 15:00	18 Aug 2010 08:38

16 Aug 2010 08:53