

April 27, 2004

MEMORANDUM TO: Ellis W. Merschoff
Chief Information Officer

FROM: Roy P. Zimmerman, Director **/RA/**
Office of Nuclear Security
and Incident Response

SUBJECT: PROJECT MANAGEMENT PLAN FOR THE SECURE VIDEO
TELECONFERENCING PROJECT

The Project Management Plan for Secure Video Teleconferencing is provided at Attachment 1 in response to your January 29, 2004, memorandum, *APPROVAL TO BEGIN IMPLEMENTATION OF SECURE VIDEO TELECONFERENCING PROJECT* (Attachment 2). This plan completes Phase 1 of the project, Project Planning, and addresses requirements for Phase 2, Installation and Implementation.

Attachments: 1. Project Management Plan
2. CIO January 29, 2004, Memorandum

CONTACTS: Mark Van Winkle, NSIR/DNS
301-415-2209

Nancy Fontaine, NSIR/DNS
301-415-1253

April 27, 2004

MEMORANDUM TO: Ellis W. Merschoff
Chief Information Officer

FROM: Roy P. Zimmerman, Director **/RA/**
Office of Nuclear Security
and Incident Response

SUBJECT: PROJECT MANAGEMENT PLAN FOR THE SECURE VIDEO
TELECONFERENCING PROJECT

The Project Management Plan for Secure Video Teleconferencing is provided at Attachment 1 in response to your January 29, 2004, memorandum, *APPROVAL TO BEGIN IMPLEMENTATION OF SECURE VIDEO TELECONFERENCING PROJECT* (Attachment 2). This plan completes Phase 1 of the project, Project Planning, and addresses requirements for Phase 2, Installation and Implementation.

Attachments: 1. Project Management Plan
2. CIO January 29, 2004, Memorandum

CONTACTS: Mark Van Winkle, NSIR/DNS
301-415-2209

Nancy Fontaine, NSIR/DNS
301-425-1253

Distribution

NSIR/DNS/ISS RF J. Corbett, OCIO M. Dimig, OCIO RidsOCIO
C. Turner, OCIO M. Cohen, NSIR RidsNSIR
J. Schaeffer, OCIO J. Tomlinson, NSIR RidsNSIRDNS

ADAMS Yes Publicly Available Non-Sensitive ML041030304 Initials mww

DOCUMENT NAME: C:\MyFiles\Copies\Project Management Plan.wpd

*see previous concurrence

C = Copy without attachment/enclosure E = Copy with attachment/enclosure N = No copy

OFFICE	NSIR/DNS/ISS		NSIR/DNS/ISS:C		NSIR/DNS		NSIR/DNS:DD	
NAME	M. Van Winkle*		A. L. Silvious*		R. Way*		D. Dorman*	
DATE	04/ 12 /04		04/ 15 /04		04/19/04		04/21/04	
OFFICE	NSIR/DNS:D		NSIR/PMDA		NSIR:D			
NAME	G. Tracy* DHD for		M. Cohen*		R. Zimmerman MFW for			
DATE	04/21/04		04/23/04		04/ 27 /04			

OFFICIAL RECORD COPY

Project Management Plan
Secure Video Teleconferencing
April 2004

TABLE OF CONTENTS

1.	INTRODUCTION	1
1.1	Background	1
1.2	Objectives	2
1.3	Scope	2
1.4	Applicable Documents	3
1.5	Document Overview	3
1.6	Stakeholders	3
1.7	Assumptions	4
1.8	Risks	5
1.8.1	Description of Risks and Mitigation Strategies	5
1.8.2	Privacy Impact Risks	7
2	PROJECT MANAGEMENT	7
2.1	Plan Phases	7
2.2	Acquisition	7
2.3	Staffing	8
2.4	Security	8
2.5	Support	8
2.6	Reporting	8
2.7	Plan Schedule	8
APPENDIXES		
	Appendix A - NRC Privacy Information Act Form	A1
	Appendix B - Service Level Agreement	B1
	Appendix C - Configuration Plan for Headquarters Operation Center	C1
	Appendix D - Statement of Work for Support Services	D1
	Appendix E - Standard Operating Procedure for Scheduling and Use	E1
	Appendix F - Training Plan	F1
	Appendix G - Risk Assessment	G1
	Appendix H - Security Plan	H1
	Appendix I - Test and Evaluation Plan	I1
	Appendix J - Contingency Plan	J1

1. INTRODUCTION

1.1 Background

Many Federal agencies have established secure video teleconferencing (SVTC) capability over the past several years to improve secure communications capabilities. Currently, the NRC does not have an SVTC network. At the NRC, non-secure VTC and non-secure multi-point teleconferencing resources are available, but classified and sensitive unclassified information may not be shown or discussed on these systems. The NRC possesses secure telephone (STU III) and secure terminal equipment (STE), however this equipment only provides secure point-to-point voice and data capability. Establishing SVTC at the NRC is essential in order to stay in step with current technology used in government, to effectively interface with regions and other Federal agencies on classified and sensitive unclassified issues, and to provide secure multi-point telecommunication capability.

This project will establish two SVTC networks from a total of 12 systems. Each system will consist of commercial-off-the-shelf (COTS) camera, coder-decoder unit, amplifier, VCR/DVD, monitors/screens, microphones, and associated equipment, along with telephone-line bridging services and approved national-security encryption devices. One of the networks will be comprised of three TS/SCI systems installed in the Sensitive Compartmented Information Facilities (SCIF) at Headquarters and Region IV. This network will be capable of connection to the Secure Video Teleconferencing System (SVTS) which is a distinct SVTC system used among specified agencies to aid with command, control, and communications at the Federal level. The NRC has received approval from the Defense Information Systems Agency (DISA) to connect to the SVTS. The remaining nine systems, one at the Headquarters Operation Center (HOC) and two each at the four regions, will make up the second network. It will be approved to the SECRET level, primarily for classified/sensitive NRC business or business with other agencies not to exceed the SECRET level. The two networks will be separate from one another and will not interconnect. This separation will be necessary to maintain the TS/SCI integrity required for connection to the SVTS. The SCIFs at headquarters are currently accredited and meet the physical security requirements for TS/SCI. The SCIF planned for Region IV has been designed to meet all requirements and will be accredited after construction is completed around May 2004.

SVTC capability will posture the NRC to more effectively and efficiently accomplish its mission. It will allow Commissioners, regional administrators, and managers the ability to participate in VTC when classified or sensitive information is shown or discussed. In addition, it will improve the capability for staff at Headquarters and regions to communicate during incidents and exercises, increasing situational knowledge and aiding decision making by NRC leaders. It will also allow the NRC to more fully interface with other Federal agencies such as the Department of Homeland Security, Department of Energy, and other Intelligence Community and Federal agencies via the SVTS.

The Office of Nuclear Security and Incident Response initiated action to establish SVTC at the NRC through the Capital Planning and Investment Control process in July 2003. An Exhibit 300 which contained the SVTC project was approved by the Office of Management and Budget in November 2003 and the Business Case for the project was approved by the Chief Information Officer in January 2004.

Some acquisition and installation activities for this project have already begun in order to quickly establish SVTC capability at the NRC. A pilot SVTC system was installed in the HOC March 19, 2004. Staff have begun evaluation and training on the HOC system.

1.2 Objectives

SVTC will posture the NRC to more effectively and efficiently carry out its mission and will help attain the following NRC strategic goals:

- Prevent radiation-related deaths and illnesses, promote the common defense and security, and protect the environment in the use of civilian nuclear reactors, source, byproduct, and special nuclear material.
- Prevent or reduce the adverse impacts from radioactive waste to the current and future public health and safety.
- Support U.S. interests in the safe and secure use of nuclear materials and in nuclear non proliferation.

In addition, SVTC capability will posture the NRC to respond to terrorist threats or attacks at NRC regulated facilities and improve communication and coordination with other Federal agencies to support homeland security activities such as enhancing the control and accountability of radiological materials to prevent their potential use in radiological dispersal devices. Other goals and objectives include:

- Enhance secure communication infrastructure to support response to radiological accidents and emergencies.
- Improve support to NRC threat assessment.
- Improve emergency response training.
- Provide SVTC capability for simultaneous and multi-point participation among Headquarters, all regions, and Federal agencies.
- Establish TS/SCI SVTC capability at the SCIFs in One White Flint, Two White Flint, and Region IV.
- Establish SECRET SVTC capability at the Headquarters Operations Center and all regions.

1.3 Scope

The scope of this project extends only to SVTC. Both SVTC networks will be self-contained with no impact on other NRC systems. The stakeholders identified in 1.6 primarily will be affected by this project. Potential users will gain an additional resource for secure communications while the Office of Administration (ADM), Office of Chief Information Officer (OCIO), the Office of Nuclear Security and Incident Response (NSIR), and regions will gain responsibilities for operation, maintenance, trouble shooting, and contract administration throughout the life cycle of the project. The Service Level Agreement (SLA) for SVTC (Appendix B) describes some OCIO and NSIR responsibilities in greater detail.

1.4 Applicable Documents

The Business Case details specific project costs, net present value comparison, and the road map to explore the possible transfer of secure telecommunications from NSIR to OCIO.

Capital asset planning for this project is found in Exhibit 300 for account 31-0200-0-1-276.

The System Security Authorization Agreement (SSAA) for this project will document the certification process and project accreditation. In addition, the SSAA will catalogue the following deliverables:

- Concept of Operation
- Configuration Management Plan
- Standard Operating Procedure for Operation and Use
- Operational Risk Assessment
- Security Plan
- Contingency Plan
- Installation/Integration Plan
- Test and Evaluation Plan
- Training Plan
- Interim Authority to Operate
- Certifications of Components and Individual Systems by Space and Naval Warfare Systems Center-Charleston (SSC-CH)
- Certification by Joint Interoperability Test Center (JITC)
- Certification by ATT
- SLA

1.5 Document Overview

This Project Management Plan communicates to the major activities and milestones required for managing the SVTC project from start to finish. It is a working document created initially as an activity within Component 1 of the System Development and Life-Cycle Management Methodology and will be updated during the life of the project.

1.6 Stakeholders

All NRC staff members with the appropriate access authorization (security clearance) and need-to-know will be permitted to use SVTC. NSIR has developed a standard operating procedure (Appendix E) to codify SVTC priorities of utilization and procedures of use. The NSIR staff views the following individuals and offices as having the greatest likelihood of using the SVTC system:

- Commissioners
- Executive Director for Operations and deputies
- The Office of Nuclear Reactor Regulation
- The Office of Nuclear Regulatory Research
- The Office of Nuclear Material Safety and Safeguards
- The Office of International Programs
- NSIR
- OCIO
- Regions

1.7 Assumptions

The NRC will support licensees when emergencies occur as part of the NRC mission. SVTC will be a useful tool for this support.

Since Federal agencies increasingly have become interdependent since September 11, 2001, in order to provide for the common defense and security of the nation, these agencies will continue to interface to the maximum extent possible to collectively provide that capability. SVTC at the NRC will improve communication and increase cohesion with other agencies.

Federal agencies will increasingly rely on SVTC as a resource for command, control, and communications as indicated by the establishment of SVTS, the current routine use of SVTC by many agencies, and its use during significant events.

A terrorist attack, accident, or natural disaster at a nuclear power plant could impact the nation's infrastructure and incite public anxiety. SVTC capability will enable the NRC to more effectively and efficiently support mitigation of any of these occurrences.

SVTC will improve effectiveness and increase communications flexibility by allowing many more people to participate in classified/sensitive meetings from multiple locations than currently possible using single-point secure-voice resources that are now available to NRC staff.

Cleared contract operators will be available since they currently operate SVTC systems with Federal agencies such as the Department of the Navy and DISA in the Washington D.C. area. The operator to be contracted by the NRC will have sufficient telecommunications and video systems expertise to support NRC requirements.

Two on-site or on-call operators will be required when two systems are simultaneously used at Headquarters (HOC and SCIF).

The geographic separation of headquarters and each region would require on-site or on-call operators for each location. A total of six operators would be needed when the Headquarters

HOC and each region were engaged in SVTC while others at headquarters simultaneously were using the SVTS in a SCIF.

SVTC must be available 24 hours a day, 7 days a week in order for the NRC to posture for nuclear incidents and national emergencies in an optimum manner. The majority of routine use will occur Monday - Friday, 0800 - 1800 EST/EDT.

On-call contract operators would not be capable of immediately establishing SVTC after normal hours, but would establish the service after arriving from their on-call status. The NRC staff would need to consider this delay when planning SVTC use and when preparing and executing response plans.

Staff at each region will operate SVTC using existing FTE until one additional FTE is authorized per region (see 2.3).

The Information Security Section (ISS) and Threat Assessment Section (TAS) will each house an SVTC system in their SCIFs. An add-shed condition is anticipated if any existing FTE is used to operate SVTC at either location. This would negatively impact the staff's ability to accomplish other intelligence, communications security, or information security work that is essential to support the Commission, Executive Director for Operations, and NSIR.

1.8 Risks

1.8.1 Description of Risks and Mitigation Strategies

The level of risk (low, medium, or high) for project elements were determined by analyzing the probability of occurrence and the severity of impact using the matrix from the National Institute of Standards and Technology, *Risk Management Guide for Information Technology Systems*.

		IMPACT SEVERITY		
		LOW (= 10)	MEDIUM (= 50)	HIGH (= 100)
P R O B A B I L I T Y	HIGH (= 1.0)	LOW $1.0 \times 10 = 10$	MEDIUM $1.0 \times 50 = 50$	HIGH $1.0 \times 100 = 100$
	MEDIUM (= 0.5)	LOW $0.5 \times 10 = 5$	MEDIUM $0.5 \times 50 = 25$	MEDIUM $0.5 \times 100 = 50$
	LOW (= 0.1)	LOW $0.1 \times 10 = 1$	LOW $0.1 \times 50 = 5$	LOW $0.1 \times 100 = 10$

Risk Scale: Low (1 - 10); Medium (>10 - 50); High (>50 - 100)

The level of risk for project elements are shown in the table that follows. Risk assessments and security management plans, as part of the **SSAA and specific site operations**, will address operational risks.

PROJECT ELEMENT	OVERALL RISK (PROBABILITY/SEVERITY)	MITIGATION STRATEGY
Availability of funds	LOW 0.1 x 10 = 1	FY 03 funds were available and committed for the purchase and installation of all systems. Funds for operation and maintenance were budgeted for FY 04 - 06.
Timeliness of procurement	LOW 0.1 x 50 = 5	Purchased COTS equipment through normal channels. Any procurement delay will not significantly impact NRC mission or project since SVTC capability currently does not exist and no potential delay longer than 90 days is probable.
Hardware and software fails to perform as expected	LOW 0.1 x 100 = 10	Acquired COTS equipment with proven performance and reliability. Contracted reputable organization with proven track record for installation of SVTC systems.
Installation delays	LOW 0.5 x 10 = 5	Maintain frequent and recurring communication with Headquarter, regional, and contractor POC's to identify constraints, limiting factors, and shortfalls. Mutually develop solutions for problems. Any delay will not significantly impact NRC mission or project since SVTC capability currently does not exist and no potential delay longer than 45 days is probable.
Approval by DISA to access SVTS	LOW 0.1 x 100 = 10	Request letter justifying need sent to DISA 2/24/04. Direct discussions indicate likelihood of approval.
SVTC component protection	LOW 0.1 x 50 = 5	Formal programs are established for inventory control, resource security, and facility surveillance. Equipment will be maintained in restricted and secure areas. Security plan will codify SOP's to minimize risk.
Encryption equipment and key protection	LOW 0.1 x 100 = 10	Formal programs are established for inventory control, resource security, and facility surveillance. Equipment and key will be maintained in restricted and secure areas. Security plan will codify SOP's to minimize risk.
Capability of agency to manage project	LOW 0.1 x 50 = 5	Integrated an NRC inter-office team with diverse skill sets to manage project.
PROJECT ELEMENT	OVERALL RISK (PROBABILITY/SEVERITY)	MITIGATION STRATEGY

Insufficient staffing	LOW 0.1 x 50 = 5	Initiated contract action for interim operators for first 12 months of systems operations. Projected .4 FTE staffing requirement and initiated hiring action 7/10/03. Will assess FTE need 4 months after fielding systems.
Abuse by staff or contractors	LOW 0.1 x 100 = 10	Access will be authorized only to NRC staff with need for use and access extremely limited to service contractors. Plans for systems use and security will codify procedures to minimize potential risk.
Technical obsolescence	LOW 0.1 x 50 = 5	Technology requirements will be monitored by service contractor and integrated management team.
System fails to improve secure telecommunication effectiveness and efficiency	LOW 0.1 x 50 = 5	Operations will be monitored by service contractor and integrated management team. Benchmark NRC's systems and processes with successful agencies to identify and correct known and potential weaknesses.

1.8.2 Privacy Impact Risks

A Privacy Information Act (PIA) assessment was accomplished using the NRC PIA Form (Appendix A). No privacy impact risk is expected with this project. Personal information such as names, social security numbers, dates of birth, addresses, telephone numbers, and etc. will not be collected, processed, stored, revealed, or disseminated via SVTC systems.

2. PROJECT MANAGEMENT

2.1 Plan Phases

The approved schedule baseline for this project has two phases.

- Phase 1 - Project Planning to be completed April 2004
- Phase 2 - Installation and Implementation to be completed November 2004

This plan completes Phase 1 of the project and addresses Phase 2 elements such as acquisition, installation, staffing, implementation, and support.

2.2 Acquisition

SSC-CH has been contracted to purchase, test, and install SVTC equipment for all locations. The NRC Communications Security Manager is responsible, and has initiated procurement action, for encryption components and key material. The Project Schedule at 2.6 shows the projected procurement, testing, and installation plan for each site.

2.3 Staffing

At Headquarters, NSIR is responsible for staffing aspects of the project that include project planning, installation, testing, operation, and maintenance through FY 2006. NSIR will use a combination of FTE and contractors to accomplish these responsibilities. The Project Schedule

at 2.6 shows tasks that must be accomplished to meet staffing requirements. Tasks include hiring two FTE and contracting for a supervisory project director, senior engineer, and facilitator/operator. Regions indicated existing FTE would be used to operate and maintain SVTC systems. However, NSIR has prepared justification for the FY 2005 budget to fund one additional FTE per region for information technology and secure telecommunication responsibilities of which SVTC would be included.

OCIO is responsible for staffing requirements associated with project consultations, reviews, and telecommunication circuits and lines as specified in the SLA at Appendix B.

ADM is responsible for staffing requirements associated with the administration of contracts throughout the life cycle of the project.

2.4 Security

Risk assessments, security management plans, contingency plans, and the SSAA will address security requirements for each SVTC location and the project in general. The Project Schedule at 2.6 shows tasks the NRC will work to meet security requirements.

2.5 Support

OCIO will provide project consultation, reviews, and telecommunication circuit and line support as specified in the SLA (Appendix B).

2.6 Reporting

NSIR will periodically report to OCIO project updates and changes for the Exhibit 300 and this Project Management Plan when necessary.

2.7 Plan Schedule

The plan that follows provides an orderly sequence of accomplishing activities in order to thoroughly complete this project. It identifies major tasks along with known or projected starting and completion dates for each task. Tasks have been organized by function or geographic location to join related activities. The sequence of accomplishing tasks may be modified as necessary in order to cope with unforeseen and emergent situations.

ID	TASK NAME	START	FINISH	DURATION	STATUS
	PROJECT PLANNING & PREPARATION				
1	Contract to Perform Site Surveys	4/1/03	4/10/03	9 days	Completed
2	Conduct Site Surveys	6/3/03	10/1/03	120 days	Completed
3	Hire 2 FTE for SVTC operation	7/10/03	12/31/04	541 days	Open
4	Deliverable: Business Case	8/1/03	11/29/03	121 days	Completed
5	Contract SSC-CH for Planning, Equipment Purchase & Installation	8/12/03	9/1/03	0 days	Completed
6	Acquire Encryption Components for HOC	8/15/03	11/10/03	92 days	Completed
7	Deliverable: Exhibit 300	8/26/03	10/31/03	67 days	Completed
8	Planning Estimates from Contractor	10/1/03	10/29/03	28 days	Completed
9	Obtain Interim Authority to Operate	1/14/04	1/27/04	13 days	Completed
10	Register HOC Site with DISN	1/14/04	1/27/04	13 days	Completed
11	Deliverable: OCIO - NSIR Service Level Agreement	1/15/04	4/12/04	87 days	Completed
12	Contract for Interim Supervisory Project Director, Senior Engineer, and Facilitator/Operator	1/26/04	5/16/04	137 days	Open
13	Establish IAA for DISN Video Services	2/3/04	4/12/04	69 days	Completed
14	Deliverable: Project Management Plan	2/11/04	4/22/04	113 days	Completed
15	Obtain Authority to Access SVTS	2/24/04	3/30/04	35 days	Completed
	HQ HOC ACQUISITION & INSTALLATION				
16	Install Physical Security Measures	10/17/03	2/27/04	123 days	Completed
17	Deliverable: Configuration Management Plan	12/23/03	1/23/04	31 days	Completed
18	Acquire SVTC Components	12/23/03	1/23/04	31 days	Completed
19	Acquire Key Material	1/9/04	1/27/04	18 days	Completed
20	Deliverable: SOP for Operations and Use	1/15/04	3/22/04	82 days	Completed
21	Deliverable: Risk Assessment	2/11/04	5/23/04	144 days	Open
22	Deliverable: Contingency Plan	2/12/04	5/30/04	151 days	Open
23	Deliverable: Test and Evaluation Plan	2/13/04	5/26/04	72 days	Open
24	SSC-CH Quality Check Components	2/17/04	3/1/04	13 days	Completed
25	Deliverable: Security Plan	2/17/04	6/3/04	124 days	Open
26	Appoint Information Systems Security Officer (HOC and HQ SCIFs)	3/1/04	3/1/04	1 day	Completed

ID	TASK NAME	START	FINISH	DURATION	STATUS
27	Deliverable: Concept of Operations for Project	3/5/04	3/8/04	3 days	Completed
28	Deliverable: Installation Plan	3/8/04	3/19/04	11 days	Completed
29	Assign System Custodian(s)	3/12/04	3/12/04	1 day	Completed
30	Install System	3/18/04	3/19/04	2 days	Completed
31	Test System with JITC	3/19/04	3/19/04	1 day	Completed
32	Deliverable: Training Plan	3/19/04	3/19/04	1 day	Completed
33	Train Users	3/19/04	3/26/04	7 days	Completed
	REGION II ACQUISITION & INSTALLATION				
34	Acquire Secret-Level SVTC Components (for all Regions)	3/22/04	5/3/04	42 days	Open
35	Acquire Key Material (for all Secret-Level systems)	1/09/04	5/10/04	119 days	Open
36	Acquire Encryption Components (for Regions & SCIFs)	8/15/03	5/10/04	270 days	Open
37	Register Site with DISN	3/26/04	3/30/04	4 days	Completed
38	Deliverable: SOP for Operations and Use	4/26/04	5/6/04	10 days	Open
39	Deliverable: Risk Assessment	4/28/04	5/11/04	13 days	Open
40	Install Physical Security Measures	4/28/04	5/14/04	16 days	Open
41	Deliverable: Contingency Plan	4/29/04	5/14/04	15 days	Open
42	Deliverable: Test and Evaluation Plan	4/30/04	5/12/04	13 days	Open
43	SSC-CH Quality Check Components	5/3/04	5/13/04	10 days	Open
44	Appoint Information Systems Security Officer	5/4/04	5/4/04	1 day	Open
45	Deliverable: Installation Plan	5/7/04	5/14/04	7 days	Open
46	Assign System Custodian(s)	5/11/04	5/11/04	1 day	Open
47	Install System	5/18/04	5/19/04	2 days	Open
48	Test System with JITC	5/19/04	5/19/04	1 day	Open
49	Deliverable: Training Plan	5/19/04	5/19/04	1 day	Open
50	Train RG II Users	5/20/04	5/20/04	1 day	Open
	HQ SCIFs ACQUISITION & INSTALLATION				
51	Acquire Key Material for HQ SCIFs	6/1/04	6/25/04	24 days	Open
52	Register Sites	6/2/04	6/11/04	9 days	Open
53	Deliverable: SOP for Operation & Use	6/4/04	6/11/04	7 days	Open
54	Deliverable: Risk Assessment	6/7/04	6/18/04	11 days	Open
ID	TASK NAME	START	FINISH	DURATION	STATUS

55	Deliverable: Contingency Plan	6/10/04	6/21/04	11 days	Open
56	Deliverable: Test and Evaluation Plan	6/14/04	6/25/04	11 days	Open
57	Contractor Quality Check Components	6/18/04	6/30/04	12 days	Open
58	Deliverable: Installation Plan	6/22/04	6/29/04	7 days	Open
59	Assign System Custodians	6/24/04	6/24/04	1 day	Open
60	Instal Systems	7/6/04	7/9/04	4 days	Open
61	Test Systems	7/8/04	7/9/04	2 days	Open
62	Deliverable: Training Plan	7/9/04	7/9/04	1 day	Open
63	Train Users	7/9/04	7/13/04	4 days	Open
	REGION I ACQUISITION & INSTALLATION				
64	Register Site with DISN	7/19/04	7/30/04	11 days	Open
65	Deliverable: SOP for Operations and Use	7/20/04	7/30/04	10 days	Open
66	Install Physical Security Measures	7/22/04	8/6/04	15 days	Open
67	Deliverable: Risk Assessment	7/22/04	8/6/04	15 days	Open
68	Deliverable: Contingency Plan	7/23/04	8/10/04	18 days	Open
69	Deliverable: Test and Evaluation Plan	7/26/04	8/13/04	18 days	Open
70	SSC-CH Quality Check Components	8/2/04	8/10/04	8 days	Open
71	Appoint Information Systems Security Officer	8/5/04	8/5/04	1 day	Open
72	Deliverable: Installation Plan	8/10/04	8/18/04	11 days	Open
73	Assign System Custodian(s)	8/12/04	8/12/04	1 day	Open
74	Install System	8/23/04	8/26/04	4 days	Open
75	Test System with JITC	8/24/04	8/26/04	2 days	Open
76	Deliverable: Training Plan	8/26/04	8/26/04	1 day	Open
77	Train Users	8/25/04	8/27/04	2 days	Open
	REGION III ACQUISITION & INSTALLATION				
78	Register Site with DISN	9/2/04	9/9/04	7 days	Open
79	Deliverable: SOP for Operations and Use	9/7/04	9/16/04	12 days	Open
80	Install Physical Security Measures	9/7/04	9/17/04	13 days	Open
81	Deliverable: Risk Assessment	9/8/04	9/17/04	11 days	Open
82	Deliverable: Contingency Plan	9/13/04	9/24/04	11 days	Open
ID	TASK NAME	START	FINISH	DURATION	STATUS
83	Deliverable: Test and Evaluation Plan	9/16/04	10/1/04	15 days	Open

84	SSC-CH Quality Check Components	9/20/04	9/29/04	9 days	Open
85	Appoint Information Systems Security Officer	9/23/04	9/23/04	1 day	Open
86	Deliverable: Installation Plan	9/28/04	10/8/04	10 days	Open
87	Assign System Custodian(s)	9/30/04	9/30/04	1 day	Open
88	Install System	10/5/04	10/6/04	2 days	Open
89	Test System with JITC	10/6/04	10/6/04	1 day	Open
90	Deliverable: Training Plan	10/6/04	10/6/04	1 day	Open
91	Train Users	10/7/04	10/7/04	1 day	Open
	REGION IV ACQUISITION & INSTALLATION				
92	Register Sites	10/12/04	10/22/04	10 days	Open
93	Deliverable: SOPs for Operations and Use	10/14/04	10/22/04	8 days	Open
94	Install Physical Security Measures	10/14/04	10/28/04	14 days	Open
95	Deliverable: Risk Assessments	10/18/04	10/29/04	11 days	Open
96	Deliverable: Contingency Plans	10/21/04	11/5/04	16 days	Open
97	Deliverable: Test and Evaluation Plans	10/25/04	11/12/04	18 days	Open
98	Contractor Quality Check Components	10/28/04	11/16/04	19 days	Open
99	Appoint Information Systems Security Officer	11/1/04	11/4/04	1 day	Open
100	Deliverable: Installation Plans	11/8/04	11/19/04	11 days	Open
101	Assign System Custodian(s)	11/12/04	11/12/04	1 day	Open
102	Install Systems	11/15/04	11/18/04	4 days	Open
103	Test Systems	11/17/04	11/18/04	2 days	Open
104	Deliverable: Training Plans	11/18/04	11/18/04	1 day	Open
105	Train Users	11/18/04	11/19/04	1 day	Open
	CERTIFICATION AND ACCREDITATION OF NETWORKS				
106	Deliverable: SSAA	1/5/04	12/1/04	330 days	Open
107	DAA Accreditation	12/1/04	12/30/04	29 days	Open
	EXPLORING POSSIBLE TRANSFER OF SECURE TELECOMMUNICATIONS FROM NSIR TO OCIO				
ID	TASK NAME	START	FINISH	DURATION	STATUS
108	OCIO and NSIR Assign Members to Transition Steering Group	9/1/04	10/1/04	30 days	Open

109	Deliverable: Steering Group Drafts Charter	10/12/04	11/1/04	19 days	Open
110	DISA Final Approval to Operate	1/3/05	1/28/05	25 days	Open
111	CIO and NSIR Director Jointly Approve Charter	11/1/04	11/19/04	18 days	Open
112	OCIO and NSIR Assign Members to Working Groups	11/19/04	12/3/04	15 days	Open
113	Deliverables: Specific Work Groups Provide Recommendations to Steering Group	12/3/04	4/9/05	127 days	Open
114	Deliverable: Steering Group Consolidates Recommendations and Reports to CIO and NSIR Director	4/9/05	5/8/04	30 days	Open
115	CIO and NSIR Director Jointly Decide Which Secure Functions Will Transfer	5/8/05	7/10/05	62 days	Open

APPENDIX A - NRC PRIVACY INFORMATION ACT FORM

OCIO 8/02

U.S. Nuclear Regulatory Commission

Privacy Impact Assessment

Date: 3/29/04

General system/application (system) information (See definitions at end of document)

1. Person completing this form:

Name	Title	Phone #	E-mail	Office
Mark Van Winkle	Special Security Officer	301-4152209	mvw	NSIR

2. System owner:

Name	Title	Phone #	E-mail	Office
Miriam Cohen	Director, PMDA	301-415-6328	mlc2	NSIR

3. Person performing privacy review:

Name	Title	Phone #	E-mail	Office
Sandra Northern 3/30/2004	Privacy Program Officer	415-6879	ssn	OCIO

Comment: No Privacy Act concerns. No system of records will be developed.

4. What is the name of this system?

Secure Video Teleconferencing (SVTC)

5. Briefly describe the purpose of this system (support of what agency function)?

To provide multi-point secure video teleconferencing capability at Headquarters and regions in order to discuss and display classified and sensitive unclassified information.

6. Does this system contain any personal information (name, social security number, date of birth, home address, etc) about individuals?

Yes ___ No X

If no, stop here and return this form to John Sullivan, OCIO, jas2@nrc.gov.
If yes, please complete remainder of form.

Data in the System

1. What type of information is being maintained in the system (financial, medical, training, personnel, etc)?

2. Source of the information in this system.

Is data being collected from the subject individual? If yes, what type(s) of data is being collected?

- 2.1 Is data on this individual being collected from other NRC files and databases for this system? If yes, identify the files and databases?

 - 2.2 Is data on this individual being collected from source(s) other than the subject individual and NRC records? If yes, what is the source(s) and what type(s) of data is being collected?

 - 2.3 How will data collected from source(s) other than the subject individual or NRC records be verified as current, accurate, and complete?
3. Are the data elements described in detail and documented? If yes, what is the name of the document?

Attributes of the Data

1. Is the use of the data both relevant and necessary for the purpose for which the system is designed ?

2. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?
 - 2.1 How will aggregated data be maintained, filed, utilized?

- 2.2 How will aggregated data be validated for relevance and accuracy?

- 3. If data is consolidated, what controls protect it from unauthorized access/use?

- 4. How will the data be retrieved?
 - 4.1 Can it be retrieved by personal identifier? If yes, explain.

- 5. What type(s) of report(s) can be produced from this system?
 - 5.1 What are the reports used for?

 - 5.2 Who has access to these reports?

Maintenance of Administrative Controls

- 1. What is the retention period of the data in this system?
 - 1.1 What are the procedures for disposition of the data at the end of the retention period?

 - 1.2 How long will produced reports be maintained?

 - 1.3 Where are the reports stored?

 - 1.4 Where are the procedures documented?

2. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

2.1 What controls will be used to prevent unauthorized monitoring?

3. Under which Privacy Act system of records (SOR) notice does this system operate (link to list of SOR available on NRC Internal Home page)? Provide number and name.

3.1 If the system is being modified, will the SOR notice require amendment or revision? Explain.

Access to the Data

1. Who will have access to the data in the system (users, managers, system administrators, developers, other)?

2. Are criteria, procedures, controls, and responsibilities regarding access documented?

3. Will users have access to all data in the system or will users access be restricted? Explain.

4. What controls are in place to prevent the misuse (e.g. browsing) of data by those having access?

5. Do other systems share data or have access to data in this system?

6. Will other agencies share data or have access to data in this system (Federal, State, Local, other)? Explain.

7. Were Privacy Act clauses cited and other regulatory measures addressed in contracts with contractors having access to this system?

Return completed Privacy Act Assessment to John Sullivan, OCIO, jas2@nrc.gov.

DEFINITIONS

Personal Information is information about an identifiable individual that may include but not be limited to:

- race, national or ethnic origin, religion, age, marital or family status
- education, medical, psychiatric, psychological, criminal, financial, or employment history
- any identification number, symbol, or other particular assigned to an individual
- name, address, telephone number, fingerprints, blood type, or DNA

Aggregation of data is the taking of various data elements and then turning them into a composite of all the data to form another type of data such as tables or data arrays, or collecting data into a single database.

Consolidation means combining data from more than one source into one system, application, or process. Existing controls for the individual parts should remain or be strengthened to ensure no inappropriate access by unauthorized individuals. However, since individual pieces of data lose their identity, existing controls may actually be diminished - e.g: a summary census report may not point at the individual respondent but rather at a class of respondents, which makes it less personal.

APPENDIX B - Service Level Agreement

Office of the Chief Information Officer
Service Level Agreement for
the Office of Nuclear Security Incident Response
Secure Video Teleconferencing
April 7, 2004

1, Executive Summary

A. Definition of

A Service Level Agreement (SLA) is a contract between two parties and defines the support relationship between the Office of the Chief Information Officer (OCIO), as the service provider, and the Office of Nuclear Security and Incident Response (NSIR), as the customer. The objective of the SLA is to present a clear, concise and measurable description of what the service provider does for the customer.

B. Summary of

This is an agreement between NSIR and OCIO for the following services that will be provided by the OCIO:

8. Technical Project Management Expertise and Guidance
9. Ongoing Maintenance for Telecommunications
10. Support for Cable Infrastructure
11. Support for Technical Issues

These services will be available to NSIR on request during standard business working hours, subject to mutual agreement.

The OCIO point of contact for these services will be George Lopez, who may be reached at 301-415-7225.

C. Caveats

Cabling diagrams for the Headquarters Incident Response Center have been provided to OCIO and installation of cabling is complete. Cabling diagrams for other Headquarters locations will be provided by NSIR to OCIO approximately 60 days prior to the start of installation at these locations.

D. Approvals

This agreement is entered into and agreed to by NSIR and the OCIO on April 2004.

signed 4/12/04
signature:
Miriam L. Cohen
NSIR, Director, PMDA

signed 4/8/04
signature:
Arnold E. Levin
OCIO, Director, ICOD

2. General Clauses

A. Goal of the Agreement

The objective of this SLA is to clarify the agreements made between NSIR and the OCIO related to support of the NSIR Secure Video Teleconferencing (SVTC) project for Headquarters. It will form the basis of requests by the NSIR Project Manager for designing, installing, operating, and maintaining the system until the system is transitioned to OCIO. The transition to OCIO is planned for FY 2007, but it may occur at an earlier date, subject to mutual agreement. This agreement defines the quality and quantity of the services to be delivered by the OCIO.

B. Parties Involved

Following are the legal entities and responsible persons in the entities that are involved in this service level agreement:

<u>Legal Entities</u>	<u>Responsible Persons</u>
NSIR	John Tomlinson, NSIR senior level support Miriam Cohen, NSIR Project Manager Mark Van Winkle, NSIR point of contact Nancy Fontaine, NSIR technical point of contact
OCIO	James Corbett, OCIO/ICOD management George Lopez, OCIO/ICOD point of contact Margie Dimig, OCIO/BPIAD point of contact

3. Duration and Validity of the Agreement

The contract period for this SLA commences April XX, 2004 and continues through the transition of the SVTC project to OCIO no earlier than September 2006.

With the mutual agreement of both parties, this contract may be

- a. modified and amended;
- b. transferred to an independent third party or entity; or
- c. terminated

In addition, it may be terminated at the request of either party after 60-days notice to the other party.

4. Responsibilities of the parties involved

NSIR is fully responsible for leading and managing the SVTC Project. These responsibilities include planning the project, acquiring the equipment and services, scheduling and managing the project activities. NSIR will sponsor the Project Management Plan. Contractor and equipment costs related to the actions and services included in this SLA will be funded by NSIR.

The OCIO will provide services as outlined in Section 3 below.

At some point in the future, NSIR responsibilities may be transferred to the OCIO. This transition is not planned to take place until September 2006 at the earliest, and will be mutually planned and agreed to by both NSIR and the OCIO.

It is understood that OCIO will prepare for transition by actively engaging with NSIR on a recurring basis (i.e., quarterly meetings) to acquire a thorough understanding of SVTC operations and program requirements. OCIO will subsequently begin necessary budget, resource, and staffing planning to prepare OCIO to fully assume SVTC responsibilities on the date of mutual agreement.

5. Guarantees, warranties and dispute handling

Both parties will mutually agree and collaboratively work out differences in the best interest of the agency.

F. Maintenance of the agreement

This agreement may be changed or amended as agreed upon by both parties.

G. Costs involved

The OCIO agrees to provide stated services to NSIR on an as requested basis without cost to NSIR. NSIR will cover costs through September 2006 for the initial installation, operation and maintenance of the project.

NSIR agrees to assume financial responsibility for any and all related contractor charges until responsibilities for SVTC are transferred to OCIO.

H. Reporting

At this time, both parties agree that additional reporting on services provided is not necessary. It is assumed that project activities will be reported within the framework of each organization's management reporting processes.

I. Measurement

At this time, both parties agree that monitoring and metrics are not necessary.

3. Services and Service Levels

At the request of the NSIR Project Manager, the OCIO will provide the following services in support of NSIR SVTC:

Service 1: Technical Project Management Expertise and Guidance

A. Service Description:

As needed, the NSIR Project Manager is encouraged to request OCIO input for specific technical reviews of project plans and contractor proposals. OCIO will provide written and oral technical input related to NSIR plans and contractor proposals for the design, installation, maintenance, operation and support of SVTC.

NSIR review requests should be submitted to George Lopez with copies to James Corbett. Because of workload considerations, mutual agreement is needed for time and format.

B. Entities Involved:

NSIR will be the recipient of the services.
OCIO will be the service delivery organization.

C. Service Levels:

Performance: on request
Timing: mutual agreement by both parties
Availability: during standard business hours
Fall-back Capabilities: none
Incident handling: not applicable

Service 2: Ongoing Maintenance for Telecommunications

6. Service Description:

The OCIO will commit to support for the specified telecommunication circuits and lines up to the demarcation point (i.e., wall jack).

The NSIR Project Manager will need to work with OCIO up-front to define and specify the needed circuits and lines for this service. Because of telecommunications vendor lead time, the OCIO requests that the circuit specifications be provided no later than 2 months in advance of actual usage.

B. Entities Involved:

NSIR will be the recipient of the services.
OCIO will be the service delivery organization.

C. Service Levels:

Performance: on request

B5

Timing: mutual agreement by both parties

Availability: during standard business hours
Fall-back Capabilities: none
Incident handling: not applicable

Service 3: Support for Cable Infrastructure

A. Service Description:

The OCIO will commit to working with the NSIR Project Manager for the installation and support of the cable infrastructure necessary to provide telecommunications services to the location of the SVTC system at Headquarters.

B. Entities Involved:

NSIR will be the recipient of the services.
OCIO will be the service delivery organization.

C. Service Levels:

Performance: on request
Timing: mutual agreement by both parties
Availability: during standard business hours
Fall-back Capabilities: none
Incident handling: not applicable

Service 4: Support for Technical Issues

A. Service Description:

The OCIO will commit to providing a point of contact to the NSIR Project Manager to act as liaison for the resolution of technical issues with OCIO provided cabling and telecommunication infrastructure.

OCIO support for these services is provided during standard business hours.

OCIO has designated Emergency Telecommunications Support Coordinators (ETSC) in support of emergency telecommunication problems related to the Incident Response Center. Should an emergency situation related to telecommunication services occur outside of business hours, the Headquarters Operations Officer may contact an ETSC for assistance.

1.6 Entities Involved:

NSIR will be the recipient of the services.
OCIO will be the service delivery organization.

C. Service Levels:

Performance: on request
Timing: mutual agreement by both parties

B6

Availability: during standard business hours
Fall-back Capabilities: none
Incident handling: not applicable

B7

APPENDIX C - CONFIGURATION PLAN FOR HEADQUARTERS OPERATION CENTER

TO BE SCANNED IN

APPENDIX D - Statement of Work for Support Services

March 21, 2004

Statement of Work
For
U.S. Nuclear Regulatory Commission
Nuclear Security and Incident Response (NSIR)
Secure Video Teleconferencing Support Services

1. INTRODUCTION

1.1 Identification

The United States Nuclear Regulatory Commission (NRC) is a federally mandated agency whose primary mission is to regulate the commercial use of nuclear materials within the United States. The NRC provides licensing and regulation of nuclear reactors and industrial research use of nuclear materials, and the possession, use, processing, handling, and disposal of nuclear materials.

The Office of Nuclear Security and Incident Response (NSIR) develops overall agency policy and provides management direction for evaluation and assessment of technical issues involving security at nuclear facilities, and is the agency safeguards and security interface with the Department of Homeland Security (DHS), the intelligence and law enforcement communities, Department of Energy (DOE), and other agencies. NSIR develops and directs the NRC program for response to incidents, and is the agency incident response interface with the DHS, Federal Emergency Management Agency (FEMA) and other Federal agencies.

2. SCOPE

NRC will be installing secure video teleconferencing (SVTC) in approximately 12 locations throughout Headquarters and our Regional Offices.

The Contractor shall provide a best level effort to maintain and operate the SVTC systems at 3 locations at Headquarters and to assist with troubleshooting SVTC at the four regional offices.

2.1 Technical Services

This task requires a best level effort for on-site telecommunications support services at NRC Headquarters as follows:

- (a) Facilitate, operate, troubleshoot, perform diagnostics, and maintenance of all secure video conference component systems and equipment.
- (b) Provide secure video teleconferencing support services including providing recommendations on installation and configuration; scheduling coordination; and transport and diagnostics of secure VTC systems and equipment. Establish secure video conferences within and outside the agency, testing secure video conferencing system as needed with participants in advance of scheduled video conferences to determine compatibility with existing NRC systems and equipment.

D1

- (c) Develop procedures manual delineating roles and responsibilities and procedures supporting NSIR operational requirements.

(d) Serve as the NRC/NSIR agent to procure all video conference system-related hardware and software needed to support the video conference system and infrastructure.

2.2 Operations and Administration

The Contractor shall follow the procedures for operating a secure VTC session that will be provided. Procedures include, but are not limited to, 1) description/summary; 2) participants; 3) bandwidth requirements; 4) special requirements; 5) issues; 6) after meeting summary.

2.2.1 Principal Period of Operation (PPO)

For this task order, the PPO is defined as 0800 to 1700 Eastern Time, Monday through Friday, excluding government holidays for NRC.

3. PROJECT MANAGEMENT

All work performed under this task shall be directed by the NRC Project Officer or designated alternates, either under the provision of the basic contract or this statement of work. New tasks may be issued through the GSA ITM/COTR for significant new development projects.

The Contractor shall manage all staff provided under this task.

The Contractor shall participate in weekly meetings with the NRC and other formal meetings as required and directed by the NRC. The Contractor shall report monthly progress and financial performance for all activities under the contract in the Monthly Technical and Financial Status Report.

3.1 Staffing

The Contractor shall provide on-call personnel with pagers so that Contractor personnel can be contacted by the NRC.

3.2 Staff Orientation

The Contractor shall educate their staff to the mission and organization of the NRC, the purpose and scope of the contract, and the Contractor's organization to accomplish the tasks in the contract. This orientation shall also ensure that Contractor staff is aware of acceptable behavior and performance standards. It shall emphasize that staff members are expected to take ownership of problems and work with the users until the problem is successfully resolved even if that involves coordinating with other Contractors or NRC organizations. One of the objectives of this orientation is to ensure the staff understands that if they are first on the scene they are the owner of the problem and therefore they are to ensure the problem is resolved to the customer's satisfaction, not just passed off to someone else for resolution.

Quality customer service, sensitivity training, or similar staff orientation plans shall be updated as the Contractor learns the NRC environment and shall be given to all new Contractor staff members throughout the life of the contract.

D2

3.2.1 Performance and Conduct

The Contractor shall perform all work under this SOW in a skillful and professional manner in accordance with the standards and practices documented and/or accepted by industry or otherwise

specified herein. The Government reserves the right to require the Contractor to remove from the project any employee the CO deems careless, is identified by competent authority as not conforming to required safety standards, or who is officially cited for performing or acting in an objectionable manner, thus effecting the work or safety of others. Such notice will be presented in writing.

3.3 Monthly Technical and Financial Status Reports

The Contractor shall submit a monthly progress report to the NRC not later than the 15th of the following month in a format to be determined. The report shall provide a summary of accomplishments and projected completion of all ongoing activities and an overview of activities planned for the following period in accordance with the SOW including the following information:

- Number of video conferences scheduled
- Number of video conferences completed
- Labor, parts and materials expended
- Event/alarm summary with recommendations, actions taken and results
- Summary of maintenance records with outage statistics that show the specific reasons for each outage, the total duration of the system outage and procedures used to restore the system
- Systems Equipment Status
- Communications Circuits Status
- Parts and materials ordered
- Parts and materials received
- Equipment sent out for repair by NRC tag number
- Equipment received from repair by NRC tag number
- NRC equipment Inventory (by NRC tag number)
- Items of Special Note
- Remarks

Included in the monthly reports shall be staff hours expended, expenditures for travel, subcontracts, equipment, and software purchased; funds spent and available on each task under the contract; and any reports deemed necessary by the NRC to monitor Contractor performance. This deliverable will be submitted in hard copy and electronic format.

D3

3.4 Quality Assurance

The NRC is very concerned that the support supplied by the Contractor shall be of the highest possible quality. To ensure the highest possible quality, the Contractor shall address quality as an implied component of all other tasks and services requested in this Statement of Work and delivered

throughout the life of the contract. The NRC's goal is to achieve 100% customer satisfaction for its users, and the Contractor shall provide support that enables this level of quality to be attained.

NRC's goal is to provide 100% customer satisfaction to its end-users, its licensees, and the general public accessing NRC systems. The Contractor shall develop and implement operating procedures designed to meet this service goal and shall develop and implement a method of measuring and tracking performance against this goal.

All Contractor activities shall be in compliance with the NRC's quality assurance goal of providing 100% customer satisfaction. Workmanship performance for all Contractor efforts shall comply with current government and industry standards delineated in Section 6 of this document.

4. Deliverables

4.1 Deliverable Items

(a) Monthly Reports (see 3.3 Monthly Technical and Financial Status Reports)

4.2 Travel and Per Diem

No travel is required unless specifically required by NSIR. All travel, (except for local travel within 20 miles) must be approved by the NRC Project Officer prior to commencement of the travel.

Travel approval must specify the following:

- Name of cities to be visited
- Number of trips to each city
- Expected length of each trip
- Number of people making each trip
- Purpose of each trip

4.3. Contractor Supplied Facilities, Supplies and Services

The Contractor shall furnish all personnel, supervision, and management required to perform under this contract. Supplies required for Contractor personnel to perform work on this contract at the Contractor's facilities shall be provided by the Contractor.

5. Government Furnished Resources

The Contractor shall identify the type, amount and time frame for any required government resources, including those listed below.

D4

5.1 Facilities, Supplies and Services

The NRC will provide on-site office space and furnishings (workstation furniture, chairs, and telephones) for Contractor personnel. Additionally, the NRC will provide other support hardware and software to include appropriate computers/workstations and network equipment and connections for all Contractor personnel located in NRC space. NRC will also provide paper, pencils and related office supplies for the on-site staff. Employees on NRC sites may use NRC copying machines and

facsimile transmission capabilities as required, on a limited, non-interfering basis and exclusively for official business.

5.2 Technical Direction

Performance of work under this contract shall be subject to the technical direction of the NRC PO who will verbally and/or in writing provide information pertaining to the technical or functional environment or to specific requirements as necessary for performance of work under this task order.

The term Technical Direction is defined to include, without limitation, the following:

- Direction to the Contractor which redirect the contract effort, shift work emphasis between work areas of tasks, require pursuit of certain lines of inquiry, fill in details or otherwise serve to accomplish contractual statement of work.
- Provision of information to the contractor which assists in the interpretation of drawings, specifications or technical portions of the work description.
- The review and approval of technical reports, drawings, specifications and technical information to be delivered by the contractor to the NRC under the contract.

5.3 Documentation

The NRC will provide the Contractor with all available documentation, software manuals, diagnostic routines, warranty information, equipment configurations and any other available information necessary to perform service under this contract. All documentation provided to the Contractor will remain the property of the NRC.

6. Administrative Considerations

6.1 NRC Project Officers

The NRC Project Officer/Contracting Officers Technical Representative (COTR) is:

Nancy R. Fontaine
Senior Secure Telecommunications Specialist
Division of Nuclear Security
Office of Nuclear Security and Incident Response
MS-O2D-15
(301) 415-1253 (Voice) - (301) 415-2190 (Fax)
Internet Address: nrf@nrc.gov

D5

6.2 Place of Performance

Work is to be performed on-site at the following government installations:

US Nuclear Regulatory Commission
Headquarters Complex
11545 & 11555 Rockville Pike
Rockville, Maryland 20852

And at additional NRC and NRC Contractor locations when appropriate to the requirements of the NRC.

6.3 Hours of Work

6.3.1 Regular Hours

Contractor personnel sufficient to meet all requirements of the Statement of Work shall be on-site from 8:00am to 5pm, Monday through Friday excluding Government Holidays. VTC support service may be required outside of regular work hours schedule.

6.3.2 On-Call Requirements

Outside of the Principal Period of Operation, the Contractor shall provide on-call personnel that can be on-site within one hour of being notified of a critical requirement. On-call personnel shall be required to use a pager and to provide return call acknowledgment notification immediately after receiving a pager request. The Contractor shall provide the NRC Project Officer with points of contact for after-hours requirements. This shall include both primary and alternate telephone numbers.

6.4 Duration of Task

The period of performance of this task shall commence immediately after award of the task through September 30, 2006 or until task is canceled by the Government. This project will be incrementally funded each FY.

6.5 Security and Privacy

6.5.1 Clearances

All personnel who are assigned to perform work for the NRC under this task will require an NRC clearance since they may have access to SECRET-Restricted Data information. Once all SVTC locations have been installed, there will be a requirement to have personnel cleared to the TOP SECRET - Sensitive Compartmented Information (TS-SCI) level. Contractor personnel assigned to this will be subject to NRC security screening requirements for access to NRC sensitive automated information systems and data, and for continuous unescorted access to NRC headquarters buildings. These requirements are described in the attached document which is hereby incorporated as part of this Task/Delivery Order.

For additional information on Security Requirements, refer to Attachment 1.

6.5.2 Privacy Act

NRC data may contain classified information and may not be disclosed to parties. Contractor personnel will be asked to sign a non-disclosure agreement as a condition of working on this contract.

6.5.3 Security Responsibilities

The Contractor shall support NRC Network Security policies, particularly in protecting passwords and limiting access to cabling closets and common carrier demarcation locations.

7. Special Instructions

7.1 General/Miscellaneous

A permanent NRC Project Officer will be established for all Government and contractor meetings, direction and product deliverables. The NRC Project Officer will be capable of providing any clarification of the requirements required for the performance of this task.

7.2 Unique Reporting Requirements

During the execution of task assignments the Contractor shall conduct, at a minimum, meetings every week between Contractor personnel and key NRC personnel. These meetings shall take place at the NRC Headquarters office.

8. Standards and References

Adherence with the current editions of the following standards and references is required:

Telecommunications Industry Association/ Electronic Industries Alliance (TIA/ EIA)

- Federal Information Processing Standards
- FED-STD 1037B Glossary of Telecommunications Terms

In accomplishing the work specified herein, the Contractor may uncover situations where referenced or non-referenced industry standards, specifications, and criteria have conflicting guidelines. In such situations, the Contractor shall be responsible for recommending to the NRC the applicable standards, specifications or criteria obtaining approval from the NRC PO before proceeding with performance.

Attachment 1 - SECURITY REQUIREMENTS

All personnel performing on this contract will be required to have a 'Q' security. Once all locations for the secure video teleconferencing system are operational, there will be a requirement to have some or all personnel be cleared for TOP SECRET - Sensitive Compartmented Information (TS-SCI). The contractor employee shall submit a completed security forms packet, including the SF-86, 'Questionnaire for National Security Positions' and fingerprint charts, through the Project Officer to Security Branch, Division of Facilities and Security, Office of Administration for review. A contractor shall not have access to classified information or systems specified under this contract until he/she is granted a 'Q' security clearance based on a favorably adjudicated Single Scope Background Investigation (SSBI) in accordance with the procedures set forth in NRC Management Directive 12.3, Part I. The individual will be subject to a reinvestigation every five years.

NSIR

Headquarters Operations Center

SECURE VIDEO TELECONFERENCING

STANDARD OPERATING PROCEDURES

TABLE OF CONTENTS

7. INTRODUCTION

- 1. Purpose
- 2. Mission
- 3. Scope
- 4. General
- 5. Encryption

1.2 RESPONSIBILITIES

- 2.1 Network Operations
- 2.2 Facility Manager
- 2.3 Customer
- 2.4 Facilitator/Operator
- 2.5 VTC Information Systems Security Officer

1.3 PROCEDURES

- 3.1 Scheduling
- 3.2 Operations
- 3.3 Session Control Panel
- 3.4 Maintenance and System Troubleshooting

1.4 SECURITY

- 4.1 Personnel Security
- 4.2 Physical Security
- 4.3 COMSEC
- 4.4 VTC System Security
- 4.5 Security Incident Reporting

Customer Conference Request Form	TAB A
DISN Video Services	TAB B
KIV-7HS Encryption Device Config. Settings	TAB C
KIV-7HS: How to Load Key Material	TAB D
Conducting an UNCLASSIFIED Video Conference	TAB E
Conducting a CLASSIFIED Video Conference	TAB F
ADTRAN Settings Configuration Menu	TAB G
Sample VTC Session Log	TAB H
SPAWARSCEN Charleston VTC Help Desk	TAB I
VTC Equipment Setup Configuration	TAB J
VTC Troubleshooting	TAB K
SVTC Cabling Diagram	TAB L

1. INTRODUCTION

1.2 Purpose

The purpose of this Standard Operating Procedure (SOP) is to define responsibilities and provide the procedures for scheduling, preparing and facilitating a successful video teleconference using the Tanberg video teleconferencing system located in the Executive Team Room, Headquarters Operations Center (HOC), Room T4-B21.

1.2 Mission

To provide NSIR staff with a reliable video teleconferencing facility capable of providing secure and non-secure conference capabilities for point-to-point and multi-point sessions with security levels classified up to US SECRET.

1.3 Scope

This SOP applies to all customers, operators and managers of the secure video teleconferencing system located in the HOC. This document provides information and procedures concerning the scheduling, operation and maintenance of the VTC system.

1.4 General

The VTC equipment is Commercial-Off-The-Shelf (COTS) and utilizes KIV-7 cryptographic equipment for secure conferencing. Capabilities include live motion video, computer graphics, videotape, document images, and data collaboration.

1.4.1 System Components

- Tanberg 2500 CODEC electronics module contains the system electronics. It processes the audio and video compression/decompression in H.320 format. The back of the electronics module provides the cable interface for connecting to other system components and the communications network.
- Two Clarity Monitors display far-end and near-end video, system menus, online help, video from a VCR, or still image snapshots. A small picture-in-picture (PIP) window can be displayed in a corner of the screen for viewing the near-end video.
- Tanberg W.A.V.E. Camera is a compact pan-tilt-zoom (PTZ) camera with an infrared signal receiver that enables you to control your video conference from the wireless remote control. **Note:** Do not move the camera manually. Use the remote control to avoid damage to the camera.
- Two Audio-Technica Ceiling Microphones are unidirectional condenser microphones that have a 180° range.
- Tanberg Infrared Remote. All system functions used during a video conference are controlled from the Tandberg infrared Remote Control. The Remote Control must have an unobstructed path to the infrared receiver located on the front of the camera.
- KIV-7HSB crypto device for secure VTC.
- Dual Mounting Rack with Power Supply.
- Blackbox AB Switch for Secure/Non-Secure Video Teleconferencing.

- Audio Video Systems Dial Isolation Module
- Crown Audio Amplifier
- Adtran ISU-512 ST IMUX
- KSI Ceiling Speaker

1.4.2 Compatibility

- Compatible with the H.320 international standard for video conferencing
- H.261 Video Algorithm
- H.221 Communications Protocol
- G.711, G.722 and G.728 Audio Algorithms
- H.243 Chair Control
- Compatible with all updated proprietary Tanberg video algorithms
- Compatible with the H.243 standard for chair control during multipoint conferences
- Compatible with the NTSC analog video format

1.4.3 Capabilities

- Unclassified or classified operation up to SECRET.
- Multipoint conferencing through the DISN Video Services Global (DVSG) hub.
- Direct point-to-point dial up via commercial ISDN phone line.
- Computer graphics display (not yet installed).
- Objects and hard copy information displayed via the document camera (not yet installed).
- Operation at data rates up to 384 Kbps.
- Full motion video of 30 frames per second at 384 Kbps or 15 fps at 128-256 Kbps.
- Picture-in-picture display of local and remote views, or, remote picture on one screen and local picture on the other screen.

1.5 Encryption

The Secure VTC system uses the KIV-7HS High-Speed encryption device for secure VTC operation. It is an encryption device capable of operating at data rates up to 1.544 Mbps. This device is handled similar to a STU-III telephone. Once loaded with the appropriate COMSEC key, the device is unclassified upon removal of the black Cryptographic Ignition Key (CIK).

2. RESPONSIBILITIES

2.1 HOC

- Be the focal point for all SECRET level VTC scheduling and coordination.
- Issue the KIV-7HS Cryptographic Ignition Key (CIK) to designated facilitators and operators
- Verify security clearances of designated facilitators and operators prior to issuing encryption device CIK

2.2 Information Security Section (ISS)

- Provide an operational VTC system in the HOC.
- Obtain a contract for a VTC facility manager and operator for the VTC system.

- Provide an individual(s) to serve as the VTC system ISSO.
- Maintain the DISN Video Services Global (DVSG) compatible COMSEC key for the KIV-7HS encryption device.
- Register the VTC system with the DISN hub.
- Develop and maintain the VTC Facility SOP.
- Provide training as required for customer-designated facilitators/operators

2.3 Customer Responsibilities

- Read this SOP and comply with its procedures and requirements
- Coordinate VTC dates and times with the distant end prior to submitting the form
- Schedule the VTC facility
- Provide the COMSEC key for classifications other than those supported by the DVSG COMSEC key
- Report all security incidents and system vulnerabilities to the ISSO
- Follow the instructions in Section 4.4 for the operation of a PC with the VTC system

2.4 Facilitator/Operator Responsibilities

- Configure the VTC system IAW this SOP prior to conducting a conference.
- Operate the VTC system during conferences
- *Return the VTC system to its unclassified configuration at the conclusion of all classified conferences IAW Tab J (Tanberg secure ISDN Operation and Setup).
- *Verbally set the session classification level with the distant end VTC site(s) participants prior to the discussion or display of classified information
- *Verify the security clearances of all local video conference participants
- *Ensure that the distant end Facilitator/Operator has verified the security clearances of all remote site participants prior to the discussion or display of classified information
- Report all security incidents and system vulnerabilities to the ISSO
- Verify the baseline configuration of the VTC system after each use to ensure customer compliance with this SOP and applicable security procedures
- Maintain a log of VTC sessions including Facilitator/Operator, session classification level, and system modes used (computer graphic injection, data collaboration, etc.) TAB N shows a sample VTC Session Log.

** Required for secure conference operations only.*

2.5 VTC Information Systems Security Officer (ISSO)

- Duties as outlined in Management Directive 12.5.
- Develop and maintain the certification and accreditation documentation (System Security Authorization Agreement) as required by DISA and NIACAP.
- Review changes to the VTC system baseline configuration and system SOP for impact to the accreditation
- Assist in the containment of classified information in the event of a compromise or suspected compromise
- Report all security incidents to the Information Systems Security Manager.

3. PROCEDURES

3.1 Scheduling

Customers are responsible for scheduling, coordinating and deconflicting conference schedules with all remote sites prior to submitting the Customer Conference Request Form (TAB A).

1. The Customer is responsible for ensuring that all conference participants entering the HOC ET room for a classified video conference have the appropriate level of clearance.
 - The Customer's designated operator will sign for the VTC remote control pad and CIK, if required, prior to the conference.
 - The facility manager will inventory the issued items after completion of a conference and clear the operator's hand receipt.
 - Customers and operators will not modify the VTC system's configuration without authorization and approval except as identified in this SOP for normal operations. The facility manager or VTC technicians are the only individuals authorized to modify the VTC system's configuration.
 - The VTC system or its components will not be removed from its designated location within the HOC ET room without prior approval and coordination of the facility manager and ISSO.

3.1.1 Point-to-Point Conference

- Customers will complete the Customer Conference Request Form located at TAB A and submit the information to the HOC at least five working days prior to the requested conference date.
- The HOC will confirm the availability of the conference and post the new request.
- The HOC will notify the customer of the confirmed reservation or schedule conflicts via e-mail or phone within 48 hours after receiving the request form.
- The customer will coordinate all technical configuration issues with the remote site.

3.1.2 Multipoint Conference

Multipoint conferences require the use of a conferencing hub in order to permit more than one remote site to participate in a video conference. Hub services are provided by DISA over the DISN Video Service network. Customers will schedule multipoint conferences using the same procedures outlined for point-to-point conferences. Customers will coordinate with their counterparts at the far ends to obtain DVSG site Ids so hub reservations can be made as soon as possible.

3.1.3 DVSG Customer Database

3.2 Operation

3.2.1 Operator Training

The facility manager will provide a VTC operator or train customers to operate the VTC system prior to the scheduled conference. If the scheduled conference is classified, the facility manager will also verify the operator's security clearance.

3.2.2 VTC System Configuration and Setup

The Operator will configure, setup, shutdown, and sanitize the VTC system IAW with SOP before and after each session. Operators will plan and schedule for a setup time of not less than 20 minutes.

3.3 Session Control Panel

The session control panel of the VTC system conforms to the International Telecommunications Union (ITU) H.243 standard as described in the VTC industry profile. The control panel is actually a function of the conference hub and appears as a menu options on the VTC monitor when the appropriate button is pressed on the VTC remote control pad. This standard permits the chairperson to pass control of a multipoint video conference to any other site participating in the same call. This standard also permits the dynamic termination of sites during a scheduled conference, selection of what remote site is visible at any given moment, and permits the chairperson to control the view of each remote site.

3.4 Maintenance and System Troubleshooting

3.4.1 Point-to-Point Conference

If a customer has a problem during a video teleconference, the first external level of support is the VTC facility manager or designated representative. If the facility manager identifies a possible hardware problem, he will notify _____ for contractor provided maintenance support at _____.

3.4.2 Multipoint Conference

The customer will notify the facility manager or designated representative if a system problem occurs during a conference. The facility manager will resolve the problem or coordinate restoration with the DVSG hub Help Desk as necessary. The DVSG hub contractor is required to provide end-to-end customer support for all multipoint conference participants. The phone number for the DISN Video Services Global Help Desk is _____. If the facility manager identifies a possible hardware problem, he will notify _____ for contractor-provided maintenance support at _____.

4.0 SECURITY

4.1 Personnel Security

4.1.1 Classified Conferences

- The Customer is responsible for verifying the security clearances of all conference participants.
- The facility manager will verify the security clearance of the operator before issuing the KIV-7HS CIK. The KIV-7HS is classified at the level of the loaded key and the CIK which may be up to the SECRET level. Separately the CIK and encryption devices are unclassified.
- Ensure that the conference room is properly sanitized for a SECRET level conference call in accordance with the procedures in Paragraph 4.2

Place the Secure/Non-Secure Switch in the SECURE position. If the call fails to connect, refer to Tab K, "VTC Troubleshooting."

Terminating a Call

At the completion of a VTC call, press the *Disconnect* button to terminate the call.

Note of Caution: Turning off the TV monitor does NOT disconnect a call. Your camera and microphone may still be on and the network still connected in a call. Far end participants can still see and hear you.

4.1.2 Unclassified Conferences

Personnel participating in unclassified conferences are not required to possess security clearances. However, personnel must meet the requirements for access to the facility IAW section 4.2 of this SOP.

Making an Unclassified Call

Place the Secure/Non-Secure Switch in the NON-SECURE position. If the call fails to connect, refer to Tab K, "VTC Troubleshooting."

Terminating a Call

At the completion of a VTC call, press the *Disconnect* button to terminate the call.

Note of Caution: Turning off the TV monitor does NOT disconnect a call. Your camera and microphone may still be on and the network still connected in a call. Far end participants can still see and hear you.

4.2 Physical Security

Prior to making a secure video conference call, care must be taken to properly sanitize the conference room for the level of security of the conference call. If required, the Executive Team (ET) room can be made secure up to the SECRET level, using the following procedures:

- Ask all non-cleared personnel and those without a need-to-know to leave the ET (T4B-21), the ET Status (T4B-19), the Team Directors (T4B-25), and the ET Chamber (T4B-23) rooms.
- Close the door leading to the ET Status Room.
- Close the sliding door leading to the Team Directors Room.
- Lower all blinds around the room.
- Ensure that the four ET monitors in the Status Room (T4B-19), and the three ET monitors in the ET Team Directors room (T4B-25) are either turned off or are being monitored by personnel with the appropriate security clearance.
- Disconnect the ET table phone from the conference system.
- Make sure the OPS Center Monitor is turned off.
- Post the "ET in Secure Mode" signs. Place monitor/guard at the doors.

- Turn off all cell phones and pagers.
- Disconnect ET Status phone (301-816-1000).

4.3 COMSEC

- The NSIR ISS Secure Communications Center, Room O2D-6, will provide a NSA-endorsed KIV-7HS encryption device and keying material for secure conference capabilities.
- The KIV-7HS encryption device is loaded and configured for use with sites compatible with the DVSG network.
- Customers are responsible for coordinating compatible COMSEC key usage and KIV-7HS encryption device configuration with their remote site when a COMSEC key other than the DVSG compatible COMSEC key is necessary. The KIV-7HS configuration settings for the VTC system are located at TAB C.

4.3.1 COMSEC Key Control

- The HQ COMSEC Custodian will accept the DVSG COMSEC KEYMAT from the issuing authority and store the key in an authorized container certified for the storage of classified cryptographic KEYMAT.
- The HQ COMSEC Custodian will issue the DVSG COMSEC key to the facility manager as required to load the KIV-7HS encryption device.
- The facility manager will return the fill device containing the DVSG COMSEC key to the HQ COMSEC Custodian immediately after loading the KIV-7HS encryption device.

4.3.2 KIV-7HS Cryptographic Ignition Key (CIK) Control

- The KIV-7HS encryption device and its associated CIK are unclassified when separated. However, the KIV-7HS will be stored IAW the appropriate regulation governing the storage of Controlled Cryptographic Items.
- The facility manager will issue the CIK to the Customer's designated operator after verification of the operator's security clearance.
- The KIV-7HS CIK will not be stored or left unattended with the encryption device at any time.
- The operator will remove the KIV-7HS CIK from the encryption device after completion of a secure video conference and will return the key to the facility manager.
- Personnel will report the loss of the KIV-7HS CIK to the facility manager and/or the HQ COMSEC Custodian immediately.

4.4 VTC System Security

- The VTC system is located in a room behind the ET Room. The door to the room has a cipher lock and should remain closed at all times during a secure conference call.

4.4.1 VCR Usage

A VCR is currently not attached to the SVTC system. If a VCR is added to the SVTC system, conferences may be recorded. The following conditions must be met to ensure computer system security during data collaboration. Deviations from the guidance outlined in this SOP must be reported to the VTC ISSO.

- When a VCR is used for playback during a VTC session of a higher classification level than the video tape (i.e., UNCLASSIFIED video tape played during a SECRET session), the video tape will be write protected or relabeled and controlled at the higher session classification level.
- When a VCR is used for recording during a classified VTC session, the tape will be handled at the classification level of the session.
- The Facilitator/Operator will review the video tape and determine whether classified information was recorded. The Facilitator/Operator may label the video tape as unclassified if the video tape contains no classified information. In all other cases, the video tape will be labeled at the classification level of the VTC session.
- Once a video tape has recorded classified information, it will ALWAYS remain marked with the appropriate classification level. NRC does not possess the capability to completely erase video tapes.

To record a video conference, make sure the VCR is set to "Line Input," place a blank tape in the VCR and press the RECORD button. The system will record video as it appears on the monitor. Both near and far end audio will be recorded.

NOTE: At the conclusion of a classified conference, VCR tapes used during the conference must be removed from the VCR, properly labeled for the level of security of the conference, and stored in a secure location.

4.4.2 Computer Graphics Display

The Facilitator/Operator will ensure all of the following conditions are met during the display of computer graphics. Deviations from the guidance listed below will be reported to the VTC ISSO.

- Customer supplied computers and media used for graphics injection will be labeled appropriately. For example, if SECRET data is transmitted during a session, the Customer's computer and any floppy disks used in that computer during the session will be labeled at least SECRET. The equipment label requirement is driven by the classification level of the data on the disks, not the operating level of the encryption device. For example, the encryption device can be operated at the SECRET classification level but only UNCLASSIFIED disks are used during a session. In this case, it is permissible to use computers and media labeled UNCLASSIFIED.
- The encryption device must be operated in the secure mode to transmit SAFEGUARDS information.
- The encryption device must be operating in the secure mode at or above the classification level of the Customer computer prior to connecting the computer to the VTC system.
- The VTC session classification level (established by verifying participant clearances and KIV-7HS operating level) will be at least as high as the computers used to inject graphics.
- The Customer computer will not be connected to a network (SLAN, ULAN, or other) while it is being utilized for graphics injection.

E10

- Customer computers with fixed hard drives and floppy disks containing U.S. classified NOFORN, OFFICIAL USE ONLY, or other sensitive but unclassified information will not be used for graphics injection during VTC sessions with NATO or foreign countries. The

Customer shall maintain separate hard and floppy disks, labeled at the appropriate level, for classified VTC sessions with NATO and foreign countries. These disks will never be used in a computer connected to a network containing U.S. classified information.

4.4.3 Data Collaboration

The Facilitator/Operator will ensure all of the following conditions are met during data collaboration. Deviations from the guidance listed below will be reported to the VTC ISSO.

- Customer supplied computers and media used for graphics injection will be labeled appropriately. For example, if SECRET data is transmitted during a session, the Customer's computer and any floppy disks used in that computer during the session will be labeled at least SECRET. The equipment label requirement is driven by the classification level of the data on the disks, not the operating level of the encryption device. For example, the encryption device can be operated at the SECRET classification level but only UNCLASSIFIED disks are used during a session. In this case, it is permissible to use computers and media labeled UNCLASSIFIED.
- The encryption device must be operated in the secure mode to transmit SAFEGUARDS information.
- The encryption device must be operating in the secure mode at or above the classification level of the Customer computer prior to connecting the computer to the VTC system.
- The VTC session classification level (established by verifying participant clearances and KIV-7HS operating level) will be at least as high as the computers used to inject graphics. For example, if the VTC session is at the SECRET level, the Customer computer and media cannot be classified higher, i.e. TOP SECRET.
- The classification levels of the Customer supplied computer and the distant end computer used for data collaboration must match EXACTLY.
- The Customer computer will not be connected to a network (SLAN, ULAN, or other) while it is being utilized for data collaboration.
- Customer computers with fixed hard drives and floppy disks containing U.S. classified NOFORN, OFFICIAL USE ONLY, or other sensitive but unclassified information will not be used for graphics injection during VTC sessions with NATO or foreign countries. The Customer shall maintain separate hard and floppy disks, labeled at the appropriate level, for classified VTC sessions with NATO and foreign countries. These disks will never be used in a computer connected to a network containing U.S. classified information.
- Files transferred into the Customer computer must be scanned for viruses using NRC approved software. The virus definition files will be the most recent version available.

4.5 Security Incident Reporting

4.5.1 The following are considered security incidents and must be reported to the VTC ISSO:

- Customer does not verify the clearances of local session participants prior to commencing the session
- E11
- Customer or facilitator/operator does not establish the session classification level and verify the clearance level of personnel at the distant end VTC site(s)
 - Discussing or transmitting classified information during a VTC session "in the clear" or at a level above what the encryption device is operating at

- Connecting computers at dissimilar classification levels via the VTC for the purpose of data collaboration. The classification levels of the Customer supplied computer and the distant end computer used for data collaboration must match EXACTLY.
- Connecting a computer to the VTC for graphics injection or data collaboration which contains NOFORN information if the VTC session includes foreign nationals.
- Customer or Facilitator/Operator fails to sanitize the VTC suite after a session

4.5.2 Incident Resolution

- The individual discovering or suspecting a security incident will take all actions necessary to prevent the further compromise of classified information. Report the incident to the VTC ISSO immediately after ensuring no further compromise will occur.
- The Facilitator/Operator responsible for the incident is the lead for retrieving classified information to the furthest extent possible. This includes contacting all affected U.S. operated VTC sites and coordinating with them to correctly secure the information. If the incident occurs with a non-U.S. operated VTC site, do not contact the site operators until after consulting with the VTC ISSO.
- The VTC ISSO is responsible for overseeing security incident resolution. In the event of an incident with a non-U.S. operated VTC site, contact the NRC ISSM before contacting the non-U.S. operated site(s).

4.5.3 Incident Reporting

- The individual discovering or suspecting a security incident has occurred will report the incident immediately to the VTC ISSO.
- The ISSO will report all security incidents to the NRC ISSM within one day of a suspected or proven compromise and within one week otherwise.

TAB A

CUSTOMER CONFERENCE REQUEST FORM

Name of Requester: _____ Phone Number of Requester: _____

Office Symbol of Requestor: _____ E-mail address of Requester: _____

Unclassified Title of VTC Conference: _____

Date of VTC: _____ Start Time of VTC: _____

Approx # of Attendees: _____ Security Classification of VTC: __ Unclassified __ SECRET
__ SECRET- RD (NRC "Q" clearance required)

Audio-Visual Support Required: _____

Hosting Site ID and POC, Phone # if other than NRC: _____

Site ID #2: _____ Site ID #3: _____

Site ID #4: _____ Site ID #5: _____

If NRC is to be the HOST of the VTC, the requestor must get DVSG site IDs from the far end participants and verify that their site can handle the security classification of the VTC. This ID is required for each site in order to make a reservation for the hub. If NRC is not the host, the requestor will be provided the DVSG site ID to pass to the host.

TAB B

DISN Video Services

1. Reservation System

DVS is an interconnected network of five hubs and a continuously growing number of dedicated and dial-up users. A key component of the DVS Network is the DVS reservation system.

An on-line DVS-Global Scheduler (DVS-GS) is available on-line at <http://disa/dtic.mil/disnvtc/> (Select "Current Customers" link; login with assigned user name and password, then select "Send a DVS Conference Request")

Video Operations Center (VOC)

Voice Requests: toll free 1-866-228-0085
(618) 229-9910

E-mail Requests: voc@scott.disa.mil

Fax Requests: (618) 229-8688

Flag Level / VIP Conferences

To ensure that AT&T, the VOC, and NS55 are aware of high-profile conferences, always indicate on your DVS Conference Request Form when Flag level and/or VIP participation is expected. Also, including the name/rank of the participating Flag/VIP in the Customer Comment section of the form would be appreciated.

On-Demand Conference Requests

VTCs that are requested **within 2 hours** of start time are defined as "On-Demand" conference requests. On-Demand conference requests, including new conferences or changes to existing conferences, must be made directly to AT&T's Video Network Management Center (VNMC). AT&T will do everything they can to accommodate On-Demand requests, subject to the availability of time and system resources. After making arrangements with AT&T, follow-up by contacting the VOIC via voice/phone/e-mail and let them know that you submitted an On-Demand request to AT&T.

AT&T's VNMC 1-800-367-8722
Hot Line 1-877-765-0328

2. Video Operations Center

In October 2002, the Video Operations Center (VOC), located at DISA CONUS, was activated to support, among other things, a consolidated DVS reservation service. To eliminate conflicts, resulting in room denials, all reservation requests must be processed through the VOC, with the exception of "On-Demand" conference requests. The VOC manages the requests, consolidates them into a conflict-free Daily Schedule, and forwards the schedule to AT&T for network configuration and management.

The VOC also monitors all conference defects, failures, and circuit related problems reported by AT&T's VNMC. The VOC provides 24 x 7 global support to the DVS customer and can be reached at:

Commercial, toll free: 1-866-228-0085
Commercial: (618) 229-9910
E-Mail: voc@scott.disa.mil

TAB C

KIV-7HS Encryption Device Configuration Settings

SETUP A		
Cik Sel	MASTER	(Master - Independent TX/RX Clocks)
Sync Sel	NR	(Non-Redundant)
Comm Sel	FDX	(Full Duplex with End Around Resync)
Data Mod	BB	(Baseband)
Data Len	SYNCH/S	(Synchronous/Synchronous Header Bypass)
TX Rate	EXT DRC	(Externally Derived Clock - 1 X Data Rate Clock)
RX Rate	EXT DRC	(Externally Derived Clock - 1 X Data Rate Clock)
TTY Mode	AUTO	(Auto Resynchronization)
I/Fctrl	PTRS and CTCS	(Forces Signals PTRS and CTCS to True) Each Option (PTRS & CTRS) must be selected individually. No single selection available for the pair.
SETUP B		
Invert	N/A	
TX Clock	contTXC	(Continuous Transmit Clock)
RX Clock	contRXC	(Continuous Receive Clock)
SyncOOS	Disable	
Idle Sel	Disable	
Auto Phs	Off	
UpdateU	Enabled	
Clocklock	Disabled	
SETUP C		
RED I/F	EIA 530	
BLK I/F	EIA 530	
FIL I/F	102/Std	(DS-102, Common Fill, Standard Keys)
FILADDR	254	

RCUADDR	31	
Display	Medium	(Medium Intensity)
Speaker	Enabled	
SETUP D		
MSTRSL V	slave	
ALGRTHM	alg 1	

TAB D

KIV-7HS: How To Load Key Material

	Loading a Traffic Encryption Key into the KIV-7 Utilizing a DTD
	Scroll to [-LOAD] and press the INITIATE button
	Scroll to [=LD X01]
	Connect the DTD to the FILL receptacle of the KIV-7
	Turn the DTD on
	Press the INITIATE button
	Observe a "Load Good" message on the KIV-7 display window
	Turn the DTD off and remove it from the KIV-7

After performing these steps, the KIV-7 is loaded with a TEK and the CIK is registered to that KIV-7. To process data with the loaded TEK, ensure that the correct key register is selected under the [-SEL KEY] menu.

TAB E

Conducting an UNCLASSIFIED Video Teleconference

Procedures marked with an asterisk () are for conference participants. The remaining procedures shall be performed by the Facilitator/Operator.*

Ensure you have read the VTC SOP and have the following items on hand:

- **Phone number(s) for the distant site if initiating the conference**
- **The phone number for the distant end technical POC**
- **The phone number for the distant end VTC facility**

- STEP 1.** Place the Secure/Non-Secure A/B Switch in the NON-SECURE position.
- STEP 2.** Using Clarity remote, press SOURCE key. It will automatically find the video mode.
- STEP 3.** Press the CONNECT key on the remote and dial number.
- STEP 4.** Wait 15-20 seconds for the system to come on-line. If synchronization fails within the 15-20 seconds, hang up and dial again.
- *STEP 5.** Begin your VTC session when the system connects with the distant end. Use the Tanberg remote to change camera position as required during the conference, and to toggle local microphone mute between on and off.

- Proceed to the following section when you have completed your conference

- *STEP 6.** At the completion of a VTC call, press the DISCONNECT button to terminate the call. **Note of Caution:** Turning off the monitors does NOT disconnect a call. Your camera and microphone may still be on and the network still connected in a call. Far end participants can still see and hear you.
- *STEP 7.** Return the infrared remote control to the VTC facility manager.

TAB F

Conducting a CLASSIFIED Video Conference

Procedures marked with an asterisk () are for conference participants. The remaining procedures shall be performed by the Facilitator/Operator.*

Ensure you have read the VTC SOP and have the following items on hand:

- The KIV-7HS Cryptographic Ignition Key (CIK)
- Phone number(s) for the distant site if initiating the conference
- The phone number for the distant end technical POC
- The phone number for the distant end VTC facility

STEP 1. Ensure the conference room is properly sanitized for a SECURE conference call. Refer to paragraph 4.2 to ensure physical security is in place.

STEP 2. Place the Secure/Non-Secure A/B Switch in the SECURE position.

STEP 3. Place the CIK in its receptacle on the KIV-7HS and rotate the key clockwise. The KIV will power on, beep once, and start its self-test.

Note: *The KIV-7HS is programmed to automatically load the COMSEC key (key X01) compatible with the DISN Video Services Global (DVSG) network. If you require the use of a different COMSEC key, contact the ISS at 301-415-2264 for assistance.*

STEP 4. Using Clarity remote, press SOURCE key. It will automatically find the video mode.

STEP 5. Press the CONNECT key on the remote and dial number.

STEP 6. Wait 15-20 seconds for the system to come on-line. If synchronization fails within the 15-20 seconds, hang up and dial again.

***STEP 7.** Begin your VTC session when the system connects with the distant end. Use the Tanberg remote to change camera position as required during the conference, and to toggle local microphone mute between on and off.

- Proceed to the following section when you have completed your conference

***STEP 8.** At the completion of a VTC call, press the DISCONNECT button to terminate the call. **Note of Caution:** Turning off the monitors does NOT disconnect a call. Your camera and microphone may still be on and the network still connected in a call. Far end participants can still see and hear you.

***STEP 9.** Return the infrared remote control to the VTC facility manager.

TAB G

ADTRAN Settings Configuration Menu

1=NETWORK OPTIONS	1= DIAL LINE	1=SWITCH TYPE	4=AT & T SESS				
		2=CALL TYPE	4=DATA 64KBPS				
		3=TERMINAL ID	SET SPID	<i>blank</i>	(CLEAR ALL SPIDS)		
			SET LDN	LDN 1			
				LDN 2			
				LDN 3			
				LDN 4			
				LDN 5			
				LDN 6			
				LDN 7	<i>blank</i>		
				LDN 8	<i>blank</i>		
		4=DIAL OPTIONS	2=RS-366				
				1=RS366 TIME	3=5 SEC OR EON		
				2=SECURITY	2=DISABLED		
		5=AUTO ANSWER	2=ENABLED				
6=CONNECT TIMEOUT	2=30 SEC (DEFAULT)						
7=CALL SCREENING	1=ANSWER ANY						
8=PASSWORDS	1=SPV PASSWORD	<i>blank</i>	(NO PASSWORD)				
	2=RDL PASSWORD	<i>blank</i>	(NO PASSWORD)				
9=MAINT SETUP	1=AUTO TRAPS						
0=CALL NUM ID	1=ENABLED						
2=LEASED LINE					N/A		
	3=S BUS TERMINIATION	1=ENABLED					
		2=DISABLED					
2=DTE OPTIONS	1=MAX BIT RATE	1=64K MODE 1					
	2=CONNECTOR TYPE	1=RS-530					
	3=530-V35 CABLE	2=DISABLE					
	4=RS366-Y CABLE	1=ENABLE					
	5=CTS OPTION	2=FOLLOW RTS					
	6=CD OPTION	2=NORMAL					
	7=DTR OPTIONS	2=IDLE WHEN OFF					
	8=DSR OPTIONS	2=OFF IDLE + TEST					
3=BONDING SETUP	1=TXINIT	4=10 SEC					
	2=TXFA	4=10 SEC (DEF)					
	3=TXADD01	6=50 SEC (DEF)					
	4=TXDEQ	6=50 SEC (DEF)					
	5=TANULL	5=20 SEC (DEF)					
	6=TCID	3=5 SEC (DEF)					
	7=STAFFER	1=0MSEC (DEF)					
	9=530 OPTIONS	N0 530 CLEAR C					

TAB H

Sample VTC Session Log

DATE _____ TIME _____ LENGTH OF CALL _____

VTC NAME ROCKVILLEIRCNR-USGOV-SC ST 368

OPERATOR NAME _____ OFFICE SYMBOL _____

PHONE NUMBER _____

CLASSIFICATION LEVEL _____ TYPE OF CALL (Secure/Non-Secure) _____

REMOTE SITE 1 _____

REMOTE SITE 2 _____

REMOTE SITE 3 _____

REMOTE SITE 4 _____

COMPUTER GRAPHICS USE YES NO

VCR USE YES NO

DATA COLLABORATION YES NO

TAB I

SPAWARSYSCEN CHARLESTON VTC HELP DESK

If you experience any VTC system and/or equipment malfunction, please contact SPAWARSYSCEN Charleston's VTC Help Desk for assistance. The SPAWARSYSCEN Help Desk can be reached via the following:

Commercial: (843) 218-4VTC (4882)

E-Mail Address: VTCDesk@spawar.navy.mil

POC: David Wagers, SPAWARSYSCEN Charleston
Code 752DW
Commercial: (843) 218-4709
Fax: (843) 218-5708
E-Mail: david.wagers@navy.mil

TAB J

VTC EQUIPMENT SETUP CONFIGURATION

CALL QUALITY	AUDIO			AUTO		
	VIDEO			AUTO		
	NATURAL VIDEO			AUTO		
	H264			AUTO		
	VGA RESOLUTIONS			AUTO		
	ADVANCED SETTINGS	AUDIO		AUTO		
		VIDEO		AUTO		
		RESOLUTION		AUTO		
		H.331		OFF		
		STATUS FORMAT		ADVANCED		
<i>Previous Menu</i>						
PRESENTATIONS	PRESENTATION MODE			NORMAL		
	DUO VIDEO QUALITY			AUTO		
	DUO VIDEO MODE			AUTO		
	DUO VIDEO NUMBER			AUTO		
	DUO VIDEO/SHOT SOURCE			CURRENT		
	AUTO-DISPLAY SNAPSHOT IMAGE			ON		
	SNAPSHOT FILTER			ON		
<i>Previous Menu</i>						
UTILITIES	AUTO ANSWER			ON + MIC OFF		
	FAR END CAMERA CONTROL			OFF		
	DUAL MONITOR			ON		
	AUTO PIP			OFF		
	WELCOME MENU			ON		
	MCU STATUS LINE			OFF		
	SYSTEM NAME		"SITE NAME"	NRC HQ IRC		
	MENU PASSWORD					
	WEB SNAPSHOTS					
	<i>Previous Menu</i>					
MCU SERVICES	THIS FUNCTION NOT ENABLED					
AUDIO SETTINGS	INPUTS	MIC 1		ON		
		MIC 2		ON		
		AUDIO 3 (AUX)		ON		
		AUDIO 4 (VCR)		ON		
		MIXER MODE		AUTO		
		LEVEL SETTINGS	MIC 1		+3db	
			MIC 2		+3Db	
			AUDIO 3 (AUX)		+9dB	
			AUDIO 4 (VCR)		+9dB	
		<i>Previous Menu</i>				
	OUTPUTS	OUT 1			ON	
		OUT 2 (AUX)			ON	
		OUT 3 (VCR)			ON	
		LEVEL SETTINGS	OUT 1		+13.5dB	
			OUT 2 (AUX)		+13.5dB	
			OUT 3 (VCR)		+13.5dB	
	<i>Previous Menu</i>					
	ECHO CONTROL	MIC 1			ON + NR	
		MIC 2			ON + NR	
		ROOM SIZE			MEDIUM (9)	
MOTION				LOW (4)		
<i>Previous Menu</i>						
AUDIO LEVELLING (AGC)	MIC 1-2			ON		
	AUDIO 3 (AUX)			ON		
	AUDIO 4 (VCR)			ON		
	RECEIVED AUDIO			OFF		
	<i>Previous Menu</i>					

	ALERT TONES & VOLUME	VIDEO CALL ALERT TONE		C	
		TELEPHONE ALERT TONE		D	
		ALERT VOLUME (0=MIN)		8	
		ALERT SPEAKER		ON	
		KEY TONES		ON	
		<i>Previous Menu</i>			
	RESTORE AUDIO DEFAULTS	DO NOT RESET			
VIDEO SETTINGS	CAMERA TRACKING MODE			NORMAL	
	DOCUMENT CAMERA			VIDEO 3	
	PC			VGA	
	FOCUS			AUTO	
	BRIGHTNESS			AUTO	
	WHITE BALANCE			AUTO	
	VIDEO NAME	VIDEO 1		MAIN CAM	
		VIDEO 2		AUX	
		VIDEO 3		DOC CAM	
		VIDEO 4		VCR	
		VGA		PC	
		<i>Previous Menu</i>			
	VGA SETTINGS	VGA OUT		DUAL	
		VGA OUT QUALITY		AUTO	
		<i>Previous Menu</i>			
	VNC SETTINGS	ADDRESS		127.0.0.1	
		DISPLAY NUMBER		0	
		PASSWORD		*****	
		<i>Previous Menu</i>			
TERMINAL SETTINGS	NETWORK	CURRENT NETWORK		EXTERNAL	
		ISDN-BRI SETTINGS	ISDN SWITCH TYPE	NATIONAL ISDN	
		LINE 1 SETUP		OFF	
			ENABLED		
			NUMBER1		
			NUMBER2		
			SPID1		
			SPID2		
			<i>Previous Menu</i>		
		LINE 2 SETUP		OFF	
			ENABLED		
			NUMBER1		
			NUMBER2		
			SPID1		
			SPID2		
			<i>Previous Menu</i>		
		LINE 3 SETUP		OFF	
			ENABLED		
			NUMBER1		
			NUMBER2		
			SPID1		
			SPID2		
			<i>Previous Menu</i>		

DIAGNOSTICS

SYSTEM INFO

CHANNEL STATUS
CALL STATUS

FALLBACK TO TELEPHONY		OFF
ACCESS CODE		OFF
ENCRYPTION		OFF
ENCRYPTION MODE		AUTO
MAX CALL LENGTH		0
NETWORK PROFILES	NAME	CALL PREFIX
1	AUTO	AUTO
2	ISDN	H.320
3	LAN	H.323
4	Blank	AUTO
5	Blank	AUTO
6	Blank	AUTO
	<i>Previous Menu</i>	
DATA PORT 1	BAUD RATE	9600
	PARITY	NONE
	DATABITS	8
	STOP BITS	1
	MODE	CONTROL
DATA PORT 2	BAUD RATE	9600
	PARITY	NONE
	DATABITS	8
	STOP BITS	1
	MODE	AUTO
	<i>Previous Menu</i>	
LANGUAGE	LANGUAGE	ENGLISH
	<i>Previous Menu</i>	
RESTORE DEFAULTS		DO NOT RESET
SOFTWARE OPTIONS	OPTIONS INSTALLED	PRESENTER
	HARDWARE S/N	00552133
	CURRENT OPTION KEY	JVAKINC
	NEW OPTION KEY	Blank
	<i>Previous Menu</i>	
MY IP ADDRESS		NONE!
SOFTWARE		E2.1 NTSC 384Kbps
OPTIONS INSTALLED		Presenter
NETWORK		RS366 DIALING
HARDWARE S/N		00552133
MAC ADDRESS		00:50:60:80:40:EC
ETHERNET SPEED		LINK DOWN
VARIES WITH EACH CALL		
H.320		
CALLS:	TRANSMIT	RECEIVE
SYSTEM NAME		
CALL RATE (KBPS)	128.0	128.0
VIDEO PROTOCOL	H263+	H263+
AUDIO PROTOCOL	G722.1	G722.1
DATA PROTOCOL	NONE	NONE
VIDEO FORMAT	SIF	SIF
VIDEO RATE (KBPS)	96.0	96.0
AUDIO RATE (KBPS)	24.0	24.0



EXIT MENU

TEST SUBSYSTEM

VIEW CURRENT SETTINGS
RESTORE DEFAULT SETTINGS
IP ADDRESS CONFLICT CHECK
Previous Menu

DATA CHANNEL/RATE	<i>MLP/6.4</i>	MLP/6.4	
ENCRYPTION STATUS	<i>OFF</i>	OFF	
ENCRYPTION CHECK MODE	--	--	
H320 FAR END LOOP		OFF	
SYSTEM SELFTEST			
Previous Menu			

TAB K

VTC TROUBLESHOOTING

PROBLEM	POSSIBLE CAUSE	CORRECTIVE ACTION
No power to the system.	<p>Main power switch on equipment power strip not turned on.</p> <p>Power strip power light does not come on.</p> <p>No power to power strip.</p>	<p>Turn power strip switch on.</p> <p>Turn ON/OFF switch on wall to on.</p> <p>Check/reset circuit breaker at power panel.</p>
No power to a single component (CODEC, Monitor, or VCR)	<p>Component power switch not turned on.</p> <p>Component power cable not plugged into equipment power strip.</p>	<p>Turn component power switch to on.</p> <p>Plug component power cable into equipment power strip.</p>
No video on monitor.	<p>Monitor input source not set correctly.</p>	<p>Use monitor source button to set monitor for correct source input (video 1, video 2, RGB1, RGB2).</p>
No local video in PIP window.	<p>Camera video cable disconnected.</p> <p>Wrong video input selected at IR Remote Control.</p>	<p>Connect camera and reboot CODEC.</p> <p>Select proper video input at the IR Remote Control.</p>
No video from far end on main screen.	<p>Distant party has no local video.</p> <p>Call connection problem.</p>	<p>Have distant end check causes/actions listed above for "no local video."</p> <p>Push <i>Disconnect</i> button on IR Remote Control and let system re-negotiate the call.</p>

PROBLEM	POSSIBLE CAUSE	CORRECTIVE ACTION
No audio at far end.	<p>Far end has a local problem.</p> <p>Near end audio is muted.</p> <p>Local microphone cable is disconnected.</p> <p>Call connection problem.</p>	<p>Have distant end check causes/actions listed for “no audio at near end.”</p> <p>Push <i>Mic Off</i> button on IR Remote Control.</p> <p>Reconnect microphone cable.</p> <p>Push <i>Disconnect</i> button on IR Remote Control and let system re-negotiate call.</p>
No audio at near end.	<p>Volume is set to low.</p> <p>Audio cable from CODEC to monitor speaker is disconnected.</p> <p>Call connection problem.</p> <p>Distant party not sending audio.</p>	<p>Turn up volume on TV to mid-range, and use IR Remote Control to control for desired level.</p> <p>Reconnect audio cable.</p> <p>Push <i>Disconnect</i> button on IR Remote Control and let system re-negotiate call.</p> <p>Have distant end check causes/actions listed for “no audio at far end.”</p>
Camera does not respond to remote control.	<p>Camera communication with CODEC interrupted.</p> <p>Camera control cable disconnected.</p> <p>Weak batteries in IR Remote Control.</p>	<p>Cycle CODEC power off/on.</p> <p>Reconnect camera cable and cycle CODEC power off/on.</p> <p>Replace batteries.</p>

PROBLEM	POSSIBLE CAUSE	CORRECTIVE ACTION
VTC system not in conference.	<p>System setup is not configured properly.</p> <p>Crypto equipment being used is not in sync or at full operation with the far end.</p> <p>Proper keymat or segment not loaded in the crypto equipment being used.</p> <p>Network problem.</p> <p>Cable problem.</p> <p>VTC system inoperable</p>	<p>On the IR Remote Control choose MENU and verify settings.</p> <p>Restart crypto being used and ensure that the KIV-7 is in sync and at full operate.</p> <p>Load the proper keymat and segment for the conference type and ensure that the KIV-7 is in sync and at full operate.</p> <p>Check Adtran 512 ST. If video and audio are not present, check possible causes below.</p> <p>Perform continuity checks on cabling between the CODEC and the Adtran 512 ST. Refer to the system installation drawings for cable numbers and connector pinouts.</p> <p>Contact the SPAWAR Charleston VTC Help Desk for assistance.</p>
VCR does not record conference.	<p>VCR is not set to Line Input.</p> <p>Cables between CODEC and VCR not connected correctly.</p>	<p>Set VCR to Line Input prior to recording a conference.</p> <p>Verify CODEC/VCR cable connections.</p>
Not able to send VCR audio/video over VTC.	<p>Wrong video input selected at IR Remote Control.</p> <p>Cables between VCR and CODEC not connected correctly.</p>	<p>Select VCR at the IR Remote Control.</p> <p>Verify cable connections. See installation drawing.</p>

APPENDIX F - TRAINING PLAN

The Training Plan for SVTC has been designated For Official Use Only. Authorized persons may obtain a copy by contacting the Office of Nuclear Security and Incident Response, Information Security Section at (301) 415-1253 or 2209.

UNDER DEVELOPMENT

APPENDIX H - SECURITY PLAN

UNDER DEVELOPMENT

APPENDIX I - TEST AND EVALUATION PLAN

UNDER DEVELOPMENT

APPENDIX J - CONTINGENCY PLAN

UNDER DEVELOPMENT

January 29, 2004

MEMORANDUM TO: Roy P. Zimmerman, Director
Office of Nuclear Security
and Incident Response

FROM: Ellis W. Merschoff **/RA/**
Chief Information Officer

SUBJECT: APPROVAL TO BEGIN IMPLEMENTATION OF SECURE VIDEO
TELECONFERENCING PROJECT

The Office of the Chief Information Officer (OCIO) has reviewed the business case for the Secure Video Teleconferencing Project. The Office of Nuclear Security and Incident Response (NSIR) submittal proposes establishment of two secure video teleconferencing networks for use by the Commissioners, managers, and regional administrators in communicating internally during incidents and exercises. It will also allow the NRC to communicate via the Federal Secure Video Teleconferencing System with other federal agencies.

Based on the input from the OCIO technical review and the informational review conducted by the Information Technology Business Council (ITBC), the business case for implementing the capability is approved. On January 2, 2004, NSIR submitted an addendum to the business case to respond to concerns raised by the OCIO technical review (see Attachment 1) and includes additional costs for installation and maintenance of circuits and hub bridging.

The baseline spending plan approved for the All-NRC alternative which establishes the secure networks is \$1,298,000 in the first year and includes .4 FTE of NSIR staff for operations support. It is anticipated that the recurring yearly costs for operations and maintenance will be \$457,000. The approved schedule baseline for planning and implementation is in two phases:

Phase 1 - Project Planning to be completed April 2004

Phase 2 - Installation and Implementation to be completed October 2004

As the sponsor office, NSIR will fund, manage, and support the project. OCIO has agreed to work with NSIR in planning discussions starting in October 2004 to explore the transfer of these responsibilities for supporting the secure video telecommunications capability from NSIR to OCIO. The CIO and Director of NSIR will establish a Steering group in October 2004 which will provide final recommendations for planning this transition. At this time, this transition is estimated to occur no sooner than September 2006.

The OCIO staff has conducted a technical review of the business case. There are concerns about operational risks and that some additional funding and operations support may be required for the project (see Attachment 1). It is recommended that NSIR work with OCIO to address the concerns to manage these risks before implementation. The OCIO will continue to

work with NSIR throughout the implementation and include NSIR requirements in future agency infrastructure planning activities.

There are security requirements that must be implemented to obtain approved security accreditation status. The OCIO, in discussions with NSIR, has determined that the Secure Video Teleconferencing Project will be considered as a major application. NSIR should follow the guidance for security planning and reporting measures detailed in the NRC Management Directive 12.5, Handbook 12.5, Part 3 and Table 3-1. This includes the required security documentation (the Security Plan, the Risk Assessment, the IT Contingency Plan, and the Security Test and Evaluation Plan), and the assignment of an Information Systems Security Officer. The system will need to complete security testing and security accreditation process prior to production use.

The business case was distributed to the ITBC for informational review and comment. The ITBC supported the project proceeding with implementation. They requested clarification regarding regional support required and recommended that procedures for using the new capability be developed and provided to Office IT Coordinators (see Attachment 2).

Please continue coordination with the Office of the Chief Information Officer, Infrastructure and Computer Operations Division (ICOD), support staff in the implementation of this project. The OCIO ICOD support contact is Mr. James Corbett, who may be reached at (301) 415-7500. He will be responsible for coordinating support through the project implementation.

cc: M. Van Winkle, NSIR
N. Fontaine, NSIR

Attachments:

1. OCIO Technical Review of Business Case for NSIR Secure Video Teleconferencing Project
2. Results of the Review of the Business Case for NSIR Secure Video Teleconferencing Project by the Information Technology Business Council (ITBC)
3. Addendum and Changes to Business Case for Secure Video Teleconferencing

OCIO Technical Review of Business Case for NSIR Secure Video Teleconferencing Project

Following are comments raised in the OCIO Technical Review of the business case.

1. Operations Support

The support for Alternative 1 is dependent on the availability and skills of forty percent of an NSIR FTE (section 2.1.1). This limited staffing introduces significant operational risk. When there is a need for additional support or technical troubleshooting, resources may be inadequate. At this time, OCIO is not staffed to provide supplemental support; the OCIO support contracts do not currently permit making contractor support available to NSIR for this project.

It is recommended that NSIR reduce this potential risk by having contract support available to back up the limited NSIR FTE.

2. Clarification of OCIO Support role

NSIR may require two kinds of technical support-- (1) telecommunications and interface support; (2) video systems operations support. The OCIO will provide technical support related to the agency telecommunications infrastructure up to the point of connection to the secure VTC system. NSIR will be dependent on NSIR staff and contractors for system-specific technical and operations support.

It is recommended that NSIR work with OCIO to review the support roles and ensure that adequate support is being planned.

3. Roles

There are two different support roles that will be needed. A Telecommunications Engineer who would coordinate telecommunications circuit requirements and conduct interface activities with the various service providers; and a VTC facilitator to assist users in the set-up and use of the systems. The Alternative 1 in the business case (all NRC) is planning an additional FTE (.4 FTE total) in NSIR to operate the three systems on an as-needed basis at headquarters and existing FTE resources in the regions to operate the system at each region. It is not clear that the planned FTE staffing will adequately cover both support roles.

It is recommended that NSIR work with OCIO to review the two different support roles and ensure that adequate support is being planned. At this time, OCIO is not staffed to provide additional support; the OCIO support contracts do not currently permit making contractor support available to NSIR or the regions for these activities.

4. Additional Costs

The business case cost breakout (section 3.1) for Alternative 1 summarizes costs for hardware, engineering & installation, and support for operation and maintenance. There may be additional costs for site preparation and installation of telecommunications circuits and the ongoing maintenance costs for the circuits.

It is recommended that NSIR work with OCIO to review the cost analysis and ensure that additional costs are included.