Final Report

Reserve Component Employment Study 2005 (RCE-05):

Joint Reserve Component Virtual Information Operations Organization (JRVIO) for Department of Defense Mission Support

Assistant Secretary of Defense for Reserve Affairs
The Joint Staff, J-1, J-3, and J-6

October 13, 2000

Office of the Secretary of Defense

Abstract and Keywords

Abstract: In the Reserve Component Employment 2005 (RCE-05) study the Secretary of Defense directed the Assistant Secretary of Defense for Reserve Affairs and the Joint Staff, J-1, J-3, and J-6 to explore the establishment of a Joint Reserve Virtual Information Operations (JRVIO) organization. The final report focused on integrating the capabilities inherent in the military and civilian acquired skills of RC personnel for use in virtual Information Operations (IO) for DOD and Joint mission support. The RCE-05 tasking also required an interim report as a long range plan for a JRVIO organization, a proof of concept test to assess the validity of a virtually integrated RC IO and IA organization, and submission of this final report to the Deputy Secretary of Defense (DEPSECDEF) for approval. DEPSECDEF approved the interim report on May 25, 2000 and the final report on October 13, 2000. The final report recommends the activation of five JRVIOs. The five JRVIOs will provide RC support to DISA, JIOC, NSA, JTF-CND, and IOTC. The report includes resourcing initiatives, initial Concepts of Operations and a phased implementation approach, as well as technology issues. Establishment of a steering group, with the charter to prepare an annual JRVIO update and report for DEPSECDEF, was also approved.

Keywords: computers, computer networks, computer security, Department of Defense (DOD), Information Assurance (IA), Information Operations (IO), Information Security (INFOSEC), Information Superiority (IS), Information Technology (IT), Joint Reserve Virtual Information Operations (JRVIO), Reserve components (RC), Reserve Component Employment 2005 study (RCE-05)

Page intentionally left blank

Contents

Figures & Tables

Executive Summary

I. **RCE-05 TASKING:** When the Secretary of Defense (SECDEF) approved *The Reserve Component Employment 2000-2005 (RCE-05) Study*, he tasked the Joint Staff (JS) J-1, J-3, and J-6 and the Assistant Secretary of Defense/Reserve Affairs (ASD/RA), in coordination with the Office of the Assistants to the Chairman of the Joint Chiefs of Staff for National Guard and Reserve Matters (OACJCS (NG&RM)), the Assistant Secretary of Defense/Command, Control, Communications and Intelligence (ASD/C3I), Defense Information Systems Agency (DISA), US Space Command (USSPACECOM), US Joint Forces Command (USJFCOM), and the Services to examine implementing a Joint Reserve Component Virtual Information Operations Organization (JRVIO) for joint operations/joint mission support.

II. **RCE-05 JRVIO STUDY GOAL:** To evaluate the effectiveness and examine the personnel management challenges associated with the establishment of an integrated, joint Reserve component (RC) information operations (IO) organization of up to 400 personnel employing virtual operations to accomplish its missions.

III. **BACKGROUND:**

A. **IO Overview:** IO, as defined in Joint Pub 3-13, *Information Operations*, are actions taken to affect adversary information and information systems while defending one's own information and information systems. IO can be viewed as having four functional areas: electronic warfare (EW), computer network operations (CNO), information protection, and perception management. The study determined that JRVIOs could virtually support (remote or reach back support) all IO and related activities with the exceptions of: physical destruction, physical security, counter-deception, counter-propaganda, counterintelligence (CI), and electronic protection. These activities were judged to be inappropriate due to the requirement for on-site participation, training and operations associated with their execution.

B. **Interim Long Range Plan (ILRP):** As directed in the RCE-05 study, the JRVIO study co-leads developed a JRVIO ILRP and forwarded it to the Deputy Secretary of Defense (DEPSECDEF) in early April 2000. The purpose of the ILRP was to recommend an operational concept upon which to structure a JRVIO and to address personnel management issues associated with the creation of a JRVIO. The ILRP was approved with the following results:

1. The operational concept adopted was the phased creation of multiple, small, independent JRVIOs under the control of the supported organizations.

2. Thirteen personnel management recommendations to enable JRVIO operations were identified and approved.

C. **JRVIO Participants:** As jointly staffed organizations with IO mission responsibilities, the following participants were identified in the ILRP as participants in the JRVIO process:

1. United States Space Command (USSPACECOM):

- Joint Information Operation Center (JIOC)
- Joint Task Force for Computer Network Defense (JTF-CND)

2. DISA
3. National Security Agency (NSA)
4. Information Operations Technology Center (IOTC)
5. Unified Command IO staff sections

IV. **PURPOSE OF THE LONG RANGE PLAN (LRP):** To provide the DEPSECDEF a final report on the JRVIO study that:

A. Notes and integrates lessons learned from the Proof of Concept (PoC) initiated under this study.

B. Proposes a Concept of Operations (CONOP) for the JRVIO.

C. Updates the ILRP personnel management recommendations with PoC field comments/lessons learned.

D. Considers technology areas that may benefit JRVIO operations.

V. **JRVIO CONOP:**

A. **Overview:** To properly accomplish the study goals, and in line with the operational concept model approved by the DEPSECDEF in the ILRP, individual supporting CONOPS were developed by the JIOC, NSA, IOTC and DISA. It should be noted that by prior agreement between USSPACECOM and DISA, all plans for the creation of a JRVIO in support of JTF-CND were handled by DISA with detailed plans to be included in the DISA JRVIO supporting CONOPS. These supporting CONOPS are included at Annex A-1. Detailed work was done to ensure that each of the JRVIO supporting CONOPS met JRVIO criteria. Review of the individual CONOPS confirmed that the JRVIO organizations would conform to the existing norms for RC support to Department of Defense (DOD) organizations. Command and control relationships were identical to those found in non-virtual RC support elements. Additionally, the structure and functions of the various independent JRVIOs demonstrated a clear intent to imbed virtual RC IO support into the existing staff elements of supported organizations. As a result, the only major difference noted between a JRVIO organization and traditional RC IO support rendered to the Active component (AC) is the JRVIO's reliance on the use of virtual operations. DEPSECDEF approval of the JRVIO CONOPs will not create new types of DOD organizations. JRVIO will be built out of the well-established Joint Table of Manpower Distribution (JTMD) staffing process and result in the stand-up or augmentation of RC support units. Supporting JRVIO CONOPs envision making maximal use of existing facilities and equipment at JRVIO initiation.

Existing RC and AC infrastructure were used to enable virtual operations. Security issues arose regarding high-level security clearances for individuals performing certain missions and access to secure facilities, systems, and information to perform specific missions. Personnel serving in the JRVIOs would be billeted against positions in the supported organizations' JTMD for drilling reservists and Joint Table of Distribution for full time RC staffing. These positions will be developed over the Future Years Defense Program (FYDP) via traditional DOD staffing processes. Active duty manday funds are required in the near term so that joint IO commands may receive RC support from other Service/RC IO commands as they attempt to meet current commitments and to initiate virtual IO/IA support operations prior to the allocation of dedicated JRVIO manpower authorizations. Unified Command IO staff sections were considered for inclusion in JRVIO planning. However, an interim determination was made that the Unified Commands largely required on-site support and were therefore not candidates for initial JRVIO organizations. This does not in any way preclude RC support to the Unified Command IO staff sections.

B. **Estimated Manpower Table**[1]**:**

JRVIO Supported Organization		**FY01**	**FY02**	**FY03**	**FY04**	**FY05**	**FY06**	**FY07**
JIOC								
Officer		**11**	**11**	**30**	**49**	**68**	**87**	**105**
Enlisted		**4**	**4**	**11**	**18**	**25**	**32**	**39**
NSA								
Officer		**6**	**6**	**11**	**16**	**21**	**26**	**31**
Enlisted		**16**	**16**	**36**	**56**	**76**	**96**	**116**
IOTC								
Officer		**3**	**3**	**9**	**15**	**21**	**27**	**30**
Enlisted		**2**	**2**	**6**	**10**	**14**	**18**	**20**
DISA (& JTF-CND)								
Officer		**40**	**40**	**90**	**90**	**90**	**90**	**90**
Enlisted		**100**	**100**	**182**	**182**	**182**	**182**	**182**
Total Drilling Manpower								
Officer		**60**	**60**	**140**	**170**	**200**	**230**	**256**
Enlisted		**122**	**122**	**235**	**266**	**297**	**328**	**357**
Total		**182**	**182**	**375**	**436**	**497**	**558**	**633**

[1] The Estimated Manpower Table reflects the requirement to use an interim, near-term "mandays" funding solution in order to initiate JRVIO operations. Drilling reserve personnel required to establish JRVIO units will be programmed by the Services from existing end strength resources in FY 03 and the out years.

C. **Estimated Funding Table**[2]**:**

		FY01	FY02	FY03	FY04	FY05	FY06	FY07
Estimated Manday $		**$2.064M**	**$2.140M**	**$1.000M**	**$875K**	**$625K**	**$500K**	**$500K**
Estimated Drilling Billet $		**$0**	**$0**	**$3.700M**	**$4.830M**	**$6.145M**	**$7.397M**	**$8.487M**
FTS Manpower								
Officer		**0**	**0**	**3**	**4**	**5**	**6**	**7**
Enlisted		**0**	**0**	**6**	**8**	**10**	**12**	**13**
Total FTS $		**$0**	**$0**	**$663K**	**$913K**	**$1.178M**	**$1.459M**	**$1.692M**
O&M $		**$0**	**$393K**	**$563K**	**$639K**	**$715K**	**$791K**	**$831K**
Total $		**$2.064M**	**$2.533M**	**$5.926M**	**$7.257M**	**$8.663M**	**$10.147M**	**$11.510M**

1. **JRVIO RC Personnel Mix:** The JRVIO RC manpower requirements are based on Joint commands' and Combat Support Agencies' estimated JRVIO requirements. The actual Service distribution of JRVIO RC manpower will depend on the JTMD process and agreements among the Office of the Chairman of the Joint Chiefs of Staff (OCJCS), the Joint commands, the Services, and RCs.

2. **Funding Management and Distribution:**

- **Personnel:** Requirements for JRVIO personnel funds will be coordinated with OASD/RA to determine Service distributions. Personnel funds comprise the bulk of requested JRVIO funding and are used to offset manpower and manday costs.

- **O&M:** JRVIO operations and maintenance funds will be distributed in coordination with OCJCS, OASD/C3I and OASD/RA to the Services to support their RC's JRVIO operations and maintenance.

- **PBD 707:** Further resourcing synergy will be gained by leveraging the infrastructure and connectivity capabilities provided for in the Joint Reserve Intelligence Program Information Assurance Program Budget Decision (PBD) 707, 22 December 1999.

VI. **PERSONNEL MANAGEMENT ISSUES:** Recommendations for personnel management actions to facilitate the implementation of a JRVIO are extracted from the text of paragraph VII of the ILRP and listed separately by issue area. The personnel recommendations are the same as those found in the ILRP, with only minor changes to the telecommuting and

[2] The Estimated Funding Table reflects the requirement to use an interim, near-term "mandays" funding solution in order to initiate JRVIO operations. Thus the required amount of dollars to purchase mandays from RC members wartraced to other units is large at JRVIO Initial Operating Capability (IOC) but declines over the FYDP as unit ownership of billets on the JTMD is established. Manpower costs shown as "Estimated Drilling Billet $" are for reference only.

accession and retention paragraphs. The interim recommendations were reviewed within the context of lessons learned from the JRVIO PoC and it was determined that no data contradicted any of the recommendations. Field comments and lessons learned only served to further validate the ILRP personnel recommendations.

A. **Military Specialty Codes:**

1. Full implementation may require revising CNO/information technology (IT) function codes to more accurately reflect CNO/IT activities.

2. This action may also include developing functional areas and special skill identifiers, to further identify CNO/IT skilled personnel.

B. **Civilian Acquired Skills:**

1. Progress must continue toward establishing an official database that will allow for the rapid retrieval of detailed information on both civilian and Service acquired CNO/IT skills. This initiative may include the following actions:

- Developing policy guidance that mandates population of the database by all RC personnel.

- Developing policy guidance that directs the Services to sustain the currency of the CNO/IT skills database.

- CINCs, Services and agencies identification of RC manpower and personnel assigned to CNO/IT functions.

- CINCs, Services and agencies develop policies, procedures, and actions to document the required CNO/IT function information in the appropriate databases.

C. **Accession and Retention:**

1. DOD establish an OSD-sponsored steering group to focus on military CNO/IT personnel issues.

2. Services examine potential policies that treat selected CNO/IT subspecialties in the same manner as medical doctors, lawyers and chaplains for waiving pay and age requirements while allowing direct commissioning.

3. Services examine potential for employing professional or bonus pay for accessing and retaining CNO/IT personnel into pay/drill status.

4. Services examine providing for responsive reclassification of military specialty codes based upon civilian acquired skills.

D. **Career Progression:**

1. Services study the feasibility and advisability of developing the means to mitigate the “up and out” and “up or out” personnel handling procedures for high demand, CNO/IT skilled personnel.

2. Services examine the implications of developing procedures to ensure that personnel assigned to the JRVIO are promoted at a rate at least equal to that for non-JRVIO personnel serving in the same career path.

E. **Performance Monitoring:** No change to current policies is deemed necessary.

F. **Security Requirements:**

1. CINCs, Services and agencies reevaluate classification requirements for IO and related activities billets in the JRVIO. Actions supporting this reevaluation should include**:**

- DOD designate individuals selected for an assignment within the JRVIO requiring a security clearance for priority handling of the security clearance determination and adjudication process.

- DOD review the current Joint Reserve Intelligence Center (JRIC) infrastructure associated security requirements in order to determine required security clearance measures needed to allow JRVIO members full utilization of the JRIC sites.

G. **Training Strategy:**

1. CINCs, Services and agencies determine training and/or certification programs for CNO/IT skills and functions. Actions supporting training and certification may include:

- Develop methods for fully documenting required mandatory CNO/IT training and/or certification programs.

- Establish procedures for conducting mandatory periodic reviews of CNO/IT training and/or certification programs.

- Develop an Advanced Distributed Learning (ADL) program, including a certification management system, for CNO/IT training and certification.

- Establish policy to allow personnel to telecommute and use ADL and web-based training for CNO/IT certification and training.

- Establish policies and procedures to waive CNO/IT training requirements when personnel can certify equivalent competencies based on civilian acquired skills.

H. **Flexible Drilling Policies:**

1. DOD review current policies to determine if changes are required to clearly permit flexible drilling in order to standardize Service utilization of this key JRVIO enabling process.

2. Concurrently, CINCs, Services and agencies must study the need to issue or revise policy guidance in line with DOD flexible drilling guidance.

I. **Telecommuting Policies:**

1. DOD review current IO telecommuting and flexible drilling policy guidance to determine whether these policies should be standardized across Services, agencies and Unified Commands. These issues may include force protection, line of duty, Unified Code of Military Justice (UCMJ), intelligence oversight training/monitoring, Law of Armed Conflict (LOAC), and time and attendance/performance monitoring.

2. CINCs, Services, agencies consider issuing policy guidance in line with DOD telecommuting guidance.

VII. **TECHNOLOGY:** In the early stages of a JRVIO organization(s), no technology obstacles associated with the proofs of concepts conducted were noted. However, while it is difficult to predict the future of technology, what is known is that technology will change. This will require operations and maintenance funding to invest in infrastructure, equipment, software, and training. Four technology areas, among many, merit further investigation and work:

A. Collaborative Planning Tools

B. Public Key Infrastructure/Multi-level Security

C. Accountability/Audit Software

D. Virtual Private Networks

Development and refinement in these four areas, along with corresponding support from DOD policy development, have the potential to modernize and institutionalize virtual operations.

VIII. **JRVIO LRP RECOMMENDATIONS:**

A. **JRVIO Activation:** DEPSECDEF approve and direct activation of JRVIO organizations as described in this LRP.

B. **JRVIO Implementation:** DEPSECDEF approve the establishment of a JRVIO Steering Group (JSG) to oversee the progress of the implementation of the JRVIO LRP.

1. **Development:** The ASD/RA, ASD/C3I, and JS Directors of J1, J3 and J6 will report back to DEPSECDEF within 45 days of final report approval with a recommendation on the JSG's organization and charter.

2. **Representation:** At a minimum JSG representation will include OASD/C3I, OASD/RA, JS, USSPACECOM, NSA, DISA, IOTC, the Services, the RCs and any other DOD element deemed necessary by the JSG leadership.

3. **Follow-on Issues:** The JSG has oversight of JRVIO follow-on issues as described in this report and has the authority to delegate responsibilities and tasks as required. In this case, oversight is defined as monitoring the progress of the follow-on actions cited in this report and providing advice to the authorities responsible for implementation and policy development. As a minimum, the JSG will maintain oversight of the following JRVIO issues:

- Refinement of the JRVIO CONOPS activities
- Enabling JRVIO technologies and equipment
- JRVIO support to the Unified Commands
- Joint command submission of JRVIO manpower requirements
- Training strategy for JRVIO personnel using model at Annex A-2
- Personnel management issues approved in the ILRP and listed in paragraph VI above

4. **Sub-committees:** The JSG is authorized to establish sub-committees to monitor follow-on issues and make appropriate recommendations.

5. **Reporting:** The JSG will update the DEPSECDEF annually through FY 04 on JRVIO implementation.

C. **JRVIO CONOPS:** DEPSECDEF accept the JRVIO CONOPS as written. Acceptance of this recommendation recognizes the following:

1. The major initial JRVIO participants will be USSPACECOM (JIOC and JTF-CND), NSA, IOTC and DISA.

2. Implementation of the JRVIO will be initiated by each of the participating Joint commands in accordance with plans at Annex A-1.

3. Each of the Joint command participants will submit JTMD establishment and/or expansion documents in the near term.

4. Approval also supports increased use of reservists in IO activities and staffs in Unified Commands, while delaying the establishment of JRVIOs at Unified Commands pending further review and comparison of virtual IO support to Unified Commanders and their staffs from either the JIOC or from organic Unified Command RC elements.

D. **Personnel Management:** DEPSECDEF endorse the personnel management recommendations previously approved as a part of the ILRP and listed in paragraph VI above.

E. **Resourcing:**

1. DEPSECDEF consider additional active duty manday funding in the Service active duty military appropriations for JRVIO implementation in FY 01 and FY 02 during the FY 02 Budget Review:

	FY 01	FY 02
Mandays	$2.064M	$2.140M
O&M	-0-	$0.393M
Total	$2.064M	$2.533M

This additional funding is required to meet near-term commitments and to initiate virtual IO/IA support operations prior to the allocation of dedicated JRVIO manpower authorizations.

2. DEPSECDEF approve additional FTS personnel for these units as the concept and requirements of the mission mature in the FY 03 Program Review or Budget Review process:

FY 03	FY04	FY05	FY06	FY07
$0.663M	$0.913M	$1.178M	$1.459M	$1.692M

Drilling RC personnel required to establish JRVIO units are expected to be programmed by the Services from existing end strength resources in FY 03 and the out years. These adjustments should be made in the FY03-07 POM process.

Note that the manpower estimate is based on current JRVIO requirements and will be updated as the requirements are refined. The estimate represents the JRVIO force mix planned for JTMD submissions from JIOC, NSA, IOTC and DISA (including JTF-CND). The JTMD review process will allow the Services to review the manpower requirements of the five JRVIO organizations and recommend if and how these requirements could be met. The JTMD process will define the force mix and the subsequent costs associated with that construct. Some Services may plan to re-mission existing manpower to meet JRVIO requirements. Re-missioning may reduce the resource requirement. Active duty manday costs will require funding for unit OPTEMPO that cannot be accommodated within the units' Annual Training (AT) and normal 48 drills.

Final Report

LONG RANGE PLAN
to Create a
Joint Reserve Component Virtual
Information Operations Organization (JRVIO)

I. **PURPOSE:** To provide the DEPSECDEF a final report in the form of a LRP on the feasibility of creating a joint (RC) virtual organization for IO joint operations and joint mission support as tasked by the (SECDEF) in *The Reserve Component Employment 2000-2005* (RCE-05) Study. This final report:

A. Notes and integrates lessons learned and field observations from the (PoC) initiated under this Study.

B. Provides a Concept of Operations (CONOPS) for the JRVIO.

C. Provides an updated report on the personnel management recommendations to enable JRVIO operations, previously recommended in the ILRP and approved by the DEPSECDEF.

D. Considers technology areas that may benefit JRVIO operations.

II. **BACKROUND:**

A. **DPG 00-05:** In April 1998, the SECDEF issued the *Fiscal Years 2000-2005 Defense Planning Guidance (DPG)*, which mandated that DOD conduct a study examining RC employment in support of the defense strategy across the full range of employment options including homeland defense, smaller-scale contingencies (SSC), and major theater wars (MTW). The DPG directed that the study:

1. Consider alternative concepts for employing RC forces in the future.

2. Review the full range of combat and support RC roles in current operational plans and assess currently planned employment.

3. Identify and assess potential RC missions in the continental United States (CONUS) and outside CONUS in peacetime and across the full spectrum of conflict, including the RC's role in the strategic reserve.

4. Develop and assess alternative employment roles and force-mix concepts, including an evaluation of costs, benefits and risks for each option.

5. Assess RC resourcing for current and recommended requirements.

B. **RCE-05 Study:** The RCE-05 study examined how to make the RC easier to access and use, and how to better train, equip, and manage it to ensure effective mission fulfillment. RCE-05 also identified key themes that emerged as particularly important to ensuring an effective future Total Force. In July 1999, SECDEF accepted the recommendations of the Chairman of the Joint Chiefs of Staff (CJCS) and DEPSECDEF and detailed 20 follow-on RCE-05 studies, reviews, and other assessments to enhance the completeness of the

document, and to pursue further study of promising integration initiatives in areas the RCE-05 study panels lacked the time or resources to analyze in depth. One of the areas directed for further study was examination of the potential costs and benefits of a JRVIO.

C. **RCE-05 Joint Reserve Virtual Information Operations Organization:** ASD/C3I, DISA, (JS), OACJCS (NG&RM), and the Services suggested concepts for the "virtual organization" that envisioned individuals with IT skills performing their duties from dispersed locations rather than working as a single consolidated unit at a specific training center. The “virtual organization” would overcome the geographic dispersion to organize, manage and accomplish its missions and tasks by using technology to connect its members electronically across communications grids and computer networks to form functional task elements. Where required, RC members of this organization would communicate with their headquarters through classified DOD information systems such as Secure Internet Protocol Router Network (SIPRNET), from existing Reserve centers or other DOD-controlled facilities located in regions where high concentrations of CNO/IT skills are established.

Members of the "virtual organization" could be drawn from the current RC personnel pool, or recruited from the civilian sector by offering CNO/IT training at DOD expense in exchange for a commitment to join the RC for a specific number of years. "Virtual organizations" could support DOD components focusing on offensive and defensive IO such as the JTF-CND. Forming a “virtual organization” may generate cost savings by enabling DOD to better recruit and retain highly skilled CNO/IT professionals for the RC, possibly reducing the need to rely on external contractor support. However, creating a "virtual organization" would present a set of unique challenges including how to monitor unit and individual performance, how to ensure sufficient security measures for unit equipment and personnel, and how to retain quality personnel over the long term.

D. **JRVIO Study Requirements:** To explore this concept, the RCE-05 study tasked the JS J-1, J-3, and J-6 Directors and ASD/RA in coordination with OACJCS (NG&RM), ASD/C3I, DISA, USSPACECOM, USJFCOM, and the Services to examine implementing a joint RC virtual organization for IO joint operations and joint mission support. The study would evaluate its effectiveness and examine how to address the personnel management challenges such a unit would pose. The study and proof of concept implementing this initiative on a small scale were to be provided to DEPSECDEF in accordance with the following guidance at TAB 3 of the RCE-05 study:

1. “By 31 March 2000, examine the personnel management issues associated with establishing a joint RC organization based on distributive (virtual) technologies, including military specialty (MOS/AFSC/NEC) balance, retention, career progression, performance monitoring technologies and policies, adequate security measures and required levels of military training. Provide an interim report to DEPSECDEF in the form of a long range plan for a joint virtual RC information operations (IO) and information assurance (IA) organization.”

Note: DEPSECDEF approved the ILRP on May 25, 2000.

2. “By 30 June 2000, conduct a proof of concept test to assess the validity of a virtually integrated RC IO and IA organization of up to 400 personnel, and submit a final report to DEPSECDEF for approval.”

E. **What Are IO:** The following is presented to frame the context within which the JRVIO study initiative has been undertaken, and to establish a common understanding regarding the nature and requirements of IO the RC may support.[3]

1. **Defining IO:** IO are actions taken to affect adversary information and information systems while defending one's own information and information systems.[4] Ultimately, the targets of IO are the human leadership and human decision making processes of an adversary or potential adversary.

- DOD draws upon many capabilities in the conduct of IO, such as: psychological operations (PSYOP), physical destruction, EW, computer network attack and defense (CNA/CND), military deception, counter-propaganda, counter-deception, IA, operations security (OPSEC), and CI. DOD's view has evolved beyond the traditional "pillars" approach, under which all elements of warfare could be interpreted as subsets of IO. The *National Military Strategy* and *Contingency Planning Guidance*, as well as the JS and Service doctrines, guide the combatant commander's application of IO by way of the Theater Engagement Plans (TEP) and Concept Plans (CONPLANs).

- IO are synchronized with related activities, such as civil affairs and international public information (which includes public affairs), to support information themes, to counter adversary propaganda, to influence foreign audiences favorably, and to inform allied and neutral audiences. It is important to note that international public information (IPI), public affairs, and civil affairs, like the military activities listed above, have objectives apart from supporting IO. They are, therefore, *not* subsets of IO, but rather *complement* IO through dissemination of accurate, factual information.

- For ease of comprehension, IO can be divided into four functional components: EW, CNO, information protection, and perception management.[5]

- As appropriate, IO include the use of physical destruction to affect adversary information systems. IO are also conducted in a manner such that their activities and messages are consistent with and/or complement the government's international public information messages.

2. **IO in Context of Military Operations:** IO do not stand on their own. Like more traditional military operations, they are an element of military power that serve the overall U.S. defense strategy, as well as specific objectives in peacetime, crisis or war. From the perspective of U.S. defense strategy, IO provide an instrument to be used in support of regional engagement to shape the international environment in ways that advance and protect U.S. interests and as an element of military operations undertaken in response to a specific crisis or conflict.

---

[3] The IO definition and vision are under refinement. The elaboration of IO as described in section II E of this report uses material current as of the publication of this report.

[4] As defined in both DOD Directive 3600.1 and Joint Pub 3-13.
Information: 1. Facts, data, or instructions in any medium or form. 2. The meaning that a human assigns to data by means of the known conventions used in their representation.
Information system: The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information.

[5] Draft ASD/C3I White Paper, *The DOD Concept for Information Operations*, Page 3.

- In supporting peacetime regional engagement, IO generate psychological effects intended to influence foreign perceptions and decision making, and thereby to promote our objectives. DOD's IO play a contributing role in shaping the regional security environment and must be integrated into the United States Government's (USG's) broader diplomatic strategy and international public information activities.

- As part of crisis operations, IO generate both physical and psychological effects intended to help achieve the immediate objectives of the military campaign and to support the overall strategic objectives guiding U.S. involvement. DOD's IO must be incorporated into CINC planning and operations at the tactical and operational levels and coordinated with the USG's overall politico-military approach at the strategic level.

  - Offensively, IO are used to influence, disrupt, deny or destroy an adversary's information, information systems and decision processes. This can be accomplished through generating physical effects (e.g., attacking a computer network) or psychological effects (e.g., dropping leaflets).

  - Defensively, IO protect our own information environment from attack. This includes protecting our information systems (e.g., CND), protecting our processes (e.g., OPSEC), and countering disinformation.

- IO can be conducted at all levels of war. IO can be applied strategically (e.g., to affect the perceptions and thus the decisions of an adversary's leadership), operationally, (e.g., to disrupt military command and control, thus degrading an adversary's war-fighting capabilities), and tactically (e.g., to suppress enemy air defenses through EW or CNA).

- IO can play a major role at the strategic level, particularly when the objective is to compel an adversary to take particular action rather than to impose a military defeat. In other conflicts, such as a major theater war, IO may play a less prominent role at the operational and tactical levels, assisting traditional military operations in securing a military victory. In all cases, IO must be carefully integrated into the overall military strategy and closely coordinated with the associated diplomacy and international public information activities.

- Physical destruction operations may be synchronized with IO, used in support of IO, or can be used in a direct IO role. For example, physical attacks can be used to disrupt the flow of information so as to reinforce a message that the USG is seeking to transmit.

- IO must be conducted consistent with the norms of our democratic society and our alliances with democratic states. While we might seek to deceive our adversaries during a conflict, we must not seek to deceive others, including our allies, international institutions and our own public. Moreover, IO like other military operations must be conducted in compliance with the laws of armed conflict.

3. **Joint Vision 2020:** The conceptual template provided by Joint Vision 2020 provides a vision for the evolution of IO as America's Armed Forces are transformed to achieve dominance across the full spectrum of military operations.

- The continued development and proliferation of information technologies will substantially change the conduct of military operations. These changes in the information environment make information superiority a key enabler of the

transformation of the operational capabilities of the joint force and the evolution of joint command and control.

- Full spectrum dominance implies that US forces can conduct operations with tailored forces that have access to and freedom to operate in all domains – space, sea, land, air and information**.**

- The transformation of the joint force to reach full spectrum dominance rests upon information superiority as a key enabler.

- The joint force must be able to take advantage of superior information, converted to superior knowledge, to achieve decision superiority – better decisions arrived at and implemented faster than an opponent can react; or in a non-combat situation, at a tempo that allows the force to shape the situation or react to changes and accomplish its mission.

- IO may evolve into a separate mission area requiring the Services to maintain appropriately trained specialists. Improvements in doctrine, organization and technology may lead to decisive outcomes resulting primarily from IO.

- Developing the capability to conduct successful operations in the information domain requires an innovative, flexible organization that can keep pace with the constant evolution of the information environment. Structuring the RC to support and, in some cases, lead this effort is critical to the achievement of this vision.

III. **ASSUMPTIONS:** The following study assumptions established the conceptual framework and design parameters governing the development of the potential structural models, personnel management procedures and resourcing options to create a JRVIO.

A. **The JRVIO study LRP is focused across the future years defense plan (FYDP).** Beyond FY2007 everything is speculative without the potential for real programmatic resourcing.

B. **A JRVIO is considered a joint organization when it directly supports a joint customer.** For the purposes of this study, the co-leads determined that any organization, whether single or multi-Service, that directly supports a joint customer should be considered a joint organization, regardless of the organizational structure or staffing mix.

C. **A JRVIO will execute the strategic and operational requirements of the joint agency.** As defined in standard joint warfighting doctrine, the component commander or Service unit performs tactical execution. Therefore, requirements for JRVIO missions and structure are based on joint strategic and operational IO requirements.

D. **A JRVIO will rely on virtual operations to perform its assigned activities and/or mission(s).** For the purposes of this study, the co-leads and working groups defined a virtual organization as a distributed organization that can meet mission requirements without a static spatial frame of reference. The absolute and relative locations of the people, regardless of job function, do not impact the ability of the organization to function, provide transparent and responsive support, and accomplish its mission. Technology is used to overcome geographic dispersion, provide management oversight and enhance situational awareness. In a sense, the term “virtual operations” has actually become an umbrella descriptor, which has nearly replaced the use of such terms as “remote, reachback, or split-based” operations.

E. **A JRVIO may reflect a combination of arrangements to achieve virtual operations.** For example, while "virtual operations" are the cornerstone of the JRVIO, this does not imply that the JRVIO need be virtual 100% of the time. It is recognized that supported Joint commanders may require that some training or administrative support be accomplished on-site. Similarly, a JRVIO could perform its virtual support in several ways, as from a common duty site, or from widely dispersed duty sites. This assumption was designed to allow maximum flexibility in the development of a JRVIO, and recognizes the fact that there cannot be a single organizational, administrative or operational template for all virtual organizations given the broad spectrum of IO. Each JRVIO will reflect a unique blend of operational concepts and personnel management techniques reflecting the optimum solutions to address the IO requirements and functions to be performed, and the specific operational requirements of the joint customer(s) for RC support.

F. **A JRVIO may employ flexible drilling to achieve operational requirements**. JRVIOs could contribute and respond successfully to a wide range of such operational requirements through the application of the "Flexible Drilling" authorities currently available in each of the Services' policy arsenals. While the formal terminology and administrative policies vary for this technique from Service to Service, each has the capacity to authorize the development of RC drill schedules that stagger the drill periods of RC personnel to accommodate an increasing range of IO requirements and operational surges. Flexible drilling indicates variation from standard drill weekend participation, in such areas as drill days, drill period segmentation, and drill location.

G. **A JRVIO may draw on all of the RC using any available accession/funding vehicles such as: Active Duty for Training (ADT), AT, Inactive Duty training (IDT), Active Duty for Special Work (ADSW) or FTS.** JRVIO development will consider multi-RC and multi-component solutions for meeting manpower requirements. Similarly, the traditional accession and funding authorities that exist to bring RC personnel to various forms of duty from FTS, to AT, and ADT, etc., represent a wide array of possibilities to assist in forming a JRVIO. Members of all the RCs and all duty funding mechanisms are considered appropriate and available to the JRVIO.

H. **When considering personnel management issues, the study will focus on virtual use of CNO/IT skill sets and specialties.** In this context, and depending on the IO and related activities to be performed, the personnel required by the JRVIO could represent a wide array of skill sets and specialties necessary for full-spectrum IO support. However, with the sole exception of the still emerging CNO/IT skill sets, the other functional skills pertinent to the full spectrum of IO represent established, traditional skills. Such traditional skill areas include: PSYOP, civil and public affairs, military deception, combat skills, OPSEC, intelligence, CI, physical and personnel security, and EW. Personnel management procedures and programs governing accession, training, retention, promotion and career progression for these traditional skill areas are already well established in each of the Services. While the creation of a JRVIO may well require some adjustments even in these areas, the skills associated with the performance of CNO functions inherent in IO such as IA, CND, vulnerability assessment, red teaming, website review and incident response are being defined and re-defined as we gain experience. Each of the Services has handled personnel management issues related to these skills differently. Some attempts are underway to identify, carve out, create and reorganize specialty and functional areas to address the CNO/IT skill sets that will meet the future requirements of the Services, warfighters and DOD for an Information Age military force, but all are still embryonic. The vast majority of work in the personnel management arena impacting the formation of JRVIOs clearly resides in these CNO/IT skills and specialties.

I. **JRVIO missions and activities can be drawn from the full spectrum of IO functions and requirements, but must be appropriate to RC operations, not normally require on-site drilling and demonstrate a clear value to the Total Force IO effort.** The concept is grounded on the potential that the RC possess an available pool of qualified specialists that can provide valuable assistance to AC elements, stretched thin to meet emerging DOD offensive and defensive IO requirements, that often were tasked without any additional resources. By adopting an operational concept centered on remote and virtual operations, joint virtual units could undertake select IO and related activities to make an immediate and positive contribution to the IO posture of DOD. Many IO and related activities are well suited to both virtual operations and the schedules characteristic of traditional RC elements. If clear and substantial wartime or crisis benefit cannot be demonstrated, the formation of a JRVIO is not warranted. In that event, the valuable personnel and material resources should be allocated where they can have a distinct and immediate impact on the joint IO posture of the DOD.

IV. **METHODOLOGY:** The following structure and processes were developed to conduct the JRVIO study and prepare the required reports to DEPSECDEF.

A. **Study Organization:** The RCE-05 Senior Steering Group (SSG) exercises oversight for the 20 follow-on studies, analyses and reports directed by SECDEF in the RCE-05 study, which include the JRVIO study. The SSG is co-chaired by the Assistant Secretary of Defense for Strategy and Threat Reduction (ASD/S&TR), the JS J-8, and the ASD/RA. The four designated JRVIO study co-leads are ASD/RA, and the JS J-1, J-3 and J-6. The JRVIO study team is co-chaired by representatives from each of the co-leads, and works in coordination with, and includes participants from OASD/C3I, DISA, USSPACECOM, USJFCOM, the Services and the RC. The JRVIO study team established sub-committees for Requirements, Manpower and Personnel, and Technology to examine the range of issues mandated by the tasking in TAB 3 of the RCE-05 study.

B. **Study Processes:** To prepare the interim and final reports, cited in paragraphs II.D.1. and II.D.2. above, the co-leads met regularly to review the progress of the three sub-committees and provide follow-on direction to study participants. The three sub-committees focused on the following areas:

1. The Requirements Sub-committee was charged with documenting joint requirements, defining potential organizational models for a JRVIO, and planning the implementation of small-scale prototyping (proof of concept) to validate the JRVIO concept.

2. The Manpower and Personnel Sub-committee was responsible for the examination of personnel management issues impacting the formation of a “virtual organization” including such items as functional skills required, skill mix options, accession, retention and career progression challenges, etc.

3. The Technology Sub-committee was charged with evaluating possible technology and resource requirements necessary to enable a “virtual organization” to accomplish its tasks. It was also directed to consider potential technology solutions to pressing personnel management issues such as individual and unit performance monitoring, and security issues related to a virtual or distributive operational concept.

C. **Workshops:** Following the conclusion of the sub-committees’ efforts to provide preliminary conceptual and organizational structure in the above issue areas, the study co-leads formulated essential elements to analyze in the JRVIO study and determined that a

concentrated data collection effort via workshops was necessary. Therefore the following workshops were conducted:

1. **PoC Workshop:** The Requirements Sub-committee developed the scope of the PoC activities. On December 14-15, 1999, the co-leads convened a workshop to match RC IO elements to potential joint customers to arrange mutually acceptable prototyping activities. Prototyping agreements were concluded covering five concept areas of the major IO virtual support activities: IA and Information Assurance Vulnerability Alerts (IAVA) compliance, computer network defense (CND), OPSEC (website review), intelligence support to IO, and RC IO support to joint exercises.

2. **LRP Workshop I:** On January 13-14, 2000, the first workshop devoted to the development and design of the LRP was conducted. Participation in this workshop focused on the joint IO agencies' requirements. The input from the participants yielded an understanding of the specific IO and related activities appropriate for RC virtual support, and an understanding of those areas in which the joint customers would welcome assistance.

3. **Personnel Management Workshop:** Armed with a preliminary operational concept for a JRVIO to provide a discussion context, the co-leads conducted a workshop on February 9-10, 2000. Participants represented the personnel, manpower, administrative, resource and fiscal management functions of OSD, JS, Services, and RC. Personnel management issues involved with conducting JRVIO operations are summarized in Paragraph VII below.

4. **LRP Workshop II:** On February 16-17, 2000, all concerned agencies met to focus on the elements of the ILRP and the LRP. A formal presentation of the proposed JRVIO study operational concept was presented for discussion, as were the results of the Personnel Management Workshop. A consensus was achieved regarding the study assumptions and the selection of the most appropriate organizational model for the JRVIO as described in the operational concept.

5. **Technology Workshop:** On May 10-11, 2000, the J6 co-lead, acting in his capacity as the Chairman of the Technology Sub-committee, convened a workshop to consider the technologies involved with the conduct of virtual IO/IA operations. Discussions focused on four major topics: multi-level security, collaborative planning tools, performance monitoring capabilities, and virtual private networks. The results of the workshop are covered in detail at Paragraph VIII.

D. **PoC:** To test the ability of RC elements to virtually support Joint commands and agencies, a small-scale prototyping effort was conducted within the study. The background, organization, analysis, observations, and recommendations of that effort are discussed below:

1. **Background:** The JRVIO PoC was mandated by SECDEF memorandum of July 16, 1999, "Follow-on Requirements to the Reserve Component Employment – 2005 (RCE 05) Study". In preparation for fulfilling this requirement, the Requirements Sub-committee selected five JRVIO PoC concept areas as most appropriate to this study. These concept areas, concentrated in the defensive IO arena, were selected based on operational appropriateness, suitability for execution by virtual operations, and potential for execution within the study's time frame. The concept areas selected were:

- IA/IAVA Compliance

- CND
- DOD Website Operations Security
- Intelligence Support to IO
- RC IO Support to Joint Exercises

2. **Task Organization:** The PoC Workshop was the critical first step in organizing this portion of the study. Task development, assignment and tracking were accomplished as follows:

- The Joint commands and Combat Support Agencies (CSAs) briefed their current involvement in IO and identified the IO activities they proposed for JRVIO PoC execution.
- The RC briefed their capabilities and identified the resources they could make available for PoC participation.
- A "RCE-05 JRVIO Proof of Concept Agreement" was provided to both the Joint command/CSAs and the RC resource providers. This form was used to document the agreements made between parties at the workshop to participate in the proof of concept.
- A total of 25 agreements were negotiated by the conclusion of the workshop. Subsequent discussions resulted in the addition of 11 agreements, the cancellation of 5 agreements and the postponement of 3 agreements. As a result, the study moved forward with a net of 28 specific IO tasks to be performed as the JRVIO PoC.
- A tracking matrix was created that grouped all tasks, by concept area, under the appropriate Joint command/CSA. These task groupings were designated as Synergized Prototypes (SYNOP). The Joint command/CSAs were tasked to render periodic reports on the progress of each of these SYNOPs.
- A series of "Info-Grams" was published by OASD/RA and distributed to all participants during the PoC. These were used to communicate information and requirements to all parties in the PoC.

3. **Analysis:** While the specific IO tasks performed as a part of the PoC were expected to provide worthwhile contributory support, PoC emphasis was on learning lessons that could be applied to the conduct of JRVIO operations. Particular analytic focus was placed on documenting lessons learned in six key areas: structure, administration, operations, resources, technology and equipment, and security. A detailed discussion of the lessons learned in each of these areas is captured in the following paragraph.

4. **PoC Field Observations:**

- **Structure:**
  - ✔ There must be a designated focal point within the supported or parent organization that is responsible for detailed mission coordination between the JRVIO and the supported organization. This focal point must serve to communicate the specifics of mission requirements from the AC operators to the

RC supporting element(s). This focal point must have overlapping coverage between the work schedules of both the AC and RC. This focal point must have RC support coordination as their primary duty. Multiple focal points may be required if the supported organization has distinct and separate missions tasked to the RC support element.

- The management of RC support is time intensive and will not work well, if at all, without full time management resources integrated into a supported command Reserve Liaison or Reserve Forces Advisor office. This office must have knowledge of Service specific administrative, training and development requirements and the resources to coordinate these requirements with the entire RC support base. The mission coordination focal point may be part of this office.

- A joint virtual unit will require greater support effort from the Reserve Liaison or Reserve Forces Advisor office than that required from a Service organized unit. Service organized units often have internal resources for administration and training as part of their manning allocation. Service organized units may also receive administration and training support from Service specific organizations mandated to assist these units.

- A large virtual organization functions best with a "Team Leader" or another type of "Virtual Management" structure. Team leaders serve as the points of contact between the supported unit focal point and the distributed RC team members. Rank of team leaders is not necessarily important; of dominant importance are their technical skills, ability to understand and effectively communicate mission requirements, and additional time available to perform management tasks.

- Billet structures of existing units must evolve to allow greater flexibility. RC personnel with valuable civilian and/or military skills cannot be accessed either because all billets for the skill code are filled or because the individual's military skill code does not fit in the unit that needs the RC member's civilian skills. Commands must be able to recruit to both military and civilian skills in order to access RC IT skill to meet mission requirements and in order not to be handcuffed by rigid MOS billet structure.

- **Administration:**

  - Service pay systems must be accommodated by currently established drill reporting procedures. While ultimate authority to certify drill performance rests with a designated command authority (usually a "unit" Commanding Officer), Service procedures allow for reporting of rescheduled or alternate drills. Certification of acceptable performance can be done by almost any responsible individual with knowledge of the work performed and forwarded to the command authority to allow reporting through normal channels.

  - Generic "Time and Attendance" software can be used to audit the efforts of RC members assigned to computer intensive tasks. RC members using government systems through point of presence (POP) dial-in can also be audited by use of server logs. However, tracking in this fashion may not account for all research and preparation (long hand/"stubby-pencil") time required for the mission. It also does not give any qualitative analysis of the time spent online.

- Use of detailed standard operating procedures (SOP), well developed tactics, techniques and procedures (TTP) and mission specific rules of engagement (ROE) are required to eliminate ambiguity concerning military and Service specific requirements, especially if RC members operate independently away from a USG facility.

- The drill schedule for RC members operating virtually must include periodic, scheduled drill periods during which the entire unit gathers together at a common location to accomplish general military training, Service specific or unit specific tasks that can only be done in person such as physical exams or physical readiness training/testing.

- Performance evaluation schemes must be developed and closely coordinated to ensure that all Service requirements are met. The scheme should ensure that all raters are of sufficient rank and have actual knowledge of the rated individual's performance to enable a fair and competitive evaluation. Cross Service ratings must be closely monitored for legitimacy and to ensure that no member is inadvertently penalized due to lack of cultural or system knowledge by the rater. This issue is the same as that facing any current AC or RC member of a Joint command.

- **Operations:**

  - The greatest benefit of RC participation is realized when a clear understanding of actual RC duties and responsibilities both before and during the mission exists. Initial face-to-face discussions should be used to explain the overall functions of the supported organization, facilitate a clear understanding of the specific mission, understand the current capabilities and limitations of the RC support element, and define the duties and responsibilities of both the AC and RC. The supported staff element and the supporting RC element should develop and agree on realistic end-state achievements (a definition of RC products and services) and measures of effectiveness (MOE) early in the process.

  - Interim quality control checks must occur during RC product development to ensure that the product is on track and meets requirements. The RC element mission chain of command and the supported organization must plan for interim quality control time, to include redirection if they see the product is developing contrary to the expected final product.

  - Maximum RC value-added is achieved when AC operators can arrange direct interface with RC operators enabled by collaborative workspace technology vice the traditional linear transmission of guidance via the chain of command and/or e-mail. Virtual communication enabled by collaborative workspace technology was successfully applied within RC tasks. It has great potential for increasing effectiveness of dispersed operators, including the facilitation of AC/RC communication.

  - AT at the supported command may be the best way for RC members to develop mission awareness, initiate RC/AC lines of communication at all levels, and begin to develop mutual trust and confidence with AC counterparts. Over time, these initial efforts should allow much more efficient and effective virtual operations and reduce the frequency (and cost) of visits required to the supported

command. Personal relations and trust must still be built into any virtual operations to become fully effective.

- Operational products (offensive and defensive) developed by both the AC and RC become quickly outmoded due to the rapidity of change within the IT community. Civilian organizations may be more nimble in refreshing the skills of their RC employees than the military. Thus RC, with their current civilian skills, may be best equipped to provide review of AC developed products and databases for update, renewal or replacement, and train military organizations on the new IT systems.

- Extensive pre-coordination, from the onset of the planning process, is required for successful virtual participation in joint exercises. Impediments to successful performance were not attributed to virtual operations but rather to lack of complete understanding of the exercise scenario and rules of engagement. Both red team and blue team functions were successfully performed in a virtual mode. Again, initial face-to-face contact between on-site and virtual elements is a requirement for success. RC elements must strive to maintain the same points of contact throughout the planning and execution phases of the exercise.

- Increased OPTEMPO by the AC generates increased requirements on RC elements involved in COMSEC, OPSEC and web security missions. The ability to quickly fund additional active duty mandays for virtual support for increased OPTEMPO should be addressed.

- Mission specific training of the RC by the supported command is critical. Maximum use should be made of ADL techniques and equipment to enhance RC mission specific training in a cost-effective manner. Mobile training teams (MTT) from the supported command would be effectively used if RC personnel can be gathered in sufficient numbers for the training time required, such as a "home station" AT.

- It should be recognized that RC mission focus might have caused erosion of full spectrum unit/individual capabilities. Attention should be paid to recent mission focus in order to determine skill set competencies (e.g., an RC organization with a photo interpretation mission focused exclusively on counter-drugs may well have lost the capability to efficiently and effectively work counter-terrorism, weapons of mass destruction (WMD), and like missions).

- A "Best Practices" network should be established, formally or informally, so that efficient operational techniques and procedures can be developed, enhanced, and institutionalized throughout the AC and RC IO community.

- **Resources:**

  - JRVIO operations are enabled via the use of available existing RC and AC infrastructure. JRIC's, Reserve centers and other USG facilities can be and were used. Administrative matters were typically handled through existing Service unit structures or existing Joint command structures.

  - There was solicitation of ROTC elements and academic institutions to become involved in some basic exercise elements. Though not implemented, it could be a

strong potential recruiting tool to develop an awareness of and interest in the IO career possibilities in the AC and RC.

- Service Reserve Personnel Centers have a link on their websites to direct interested personnel to the Worldwide Basic Information Library (WBIL) website. The same "marketing tool" might be used to attract IT professionals to IO units whether joint or Service sponsored.

- Use of existing infrastructure, in particular JRIC sites, presented some problems of accessibility. AC or civilian personnel are required to open and close buildings and to control access and operations. Established staffing schedules at JRIC sites did not always adequately support JRVIO operations.

- Dependence on a totally unique skill set should be avoided. Access to a single RC member at the exact time and place required for AC mission support cannot be guaranteed. Ensure mission tasks that require RC support can be handled by a fairly common skill set or by multiple RC personnel with complementary skill sets.

- Ability to fund pay and allowances and travel costs for RC members for training and mission orientation varied widely from command to command and Service to Service.

- Virtual drilling allowed access to RC members with required specialties who would not otherwise have been geographically available to the supported command.

- **Technology and Equipment:**

  - Equipment and facility issues must be addressed prior to assigning individuals to perform a mission on a specified system or at a designated site. Connectivity requirements must be thoroughly researched to ensure that all systems, access permissions, interoperability and bandwidth required for the mission is available, functional and supported. Coordination may involve supported command, supporting command and one or more third parties responsible for portions of the infrastructure. It may be difficult to find the proper authority to compel action to resolve impediments.

  - Most issues ascribed to technology are actually resource issues. Technology and equipment are available that could enable JRVIO operations. However, procurement, installation and training have not been justified or budgeted.

  - Dedicated "closed loop" systems may be needed for exercises and for vulnerability analysis. Aggressive red team activity or blue team defense on an active information system could cause temporary or long term collateral damage unanticipated by the exercise design. Testing of offensive or defensive tools on an active system could also have negative collateral effects. Each Joint command that conducts IO or joint exercises that use IO should have available a dedicated, "closed loop" network. This dedicated IO laboratory should have a breadth and depth of operating systems, applications programs, hardware switches, etc. thereby becoming a cost effective and safe way to conduct both analysis and exercises without collateral damage to active systems. If such facilities exist currently, access and use issues should be coordinated.

- Collaborative workspace technology was employed successfully. However, it is server-based technology that requires a level of system administration to ensure availability. This would best be collocated with existing hardware and infrastructure, such as at JRIC's, to leverage existing system administration resources.

- Government owned equipment and government sponsored connectivity (such as the open source intelligence system (OSIS) will be required for RC members operating independent of USG facilities. JRVIO operations conducted from non-USG facilities will be conducted through an intermediate government owned server, thereby creating virtual USG locations. Legal responsibilities, (e.g. intelligence oversight rules governing the use of private equipment and private connectivity) must be thoroughly researched. Telecommuting precedents within DOD and other USG agencies might not fully cover the eventualities of IO missions, including force protection from adversary retaliation. SOPs, TTPs and ROE, involving appropriate training and legal counsel, should guide activity in this area.

- **Security:**

  - Security requirements from being "read into the program" to mission execution must be considered prior to assigning personnel. Even though the RC IO mission may be at an unclassified level, the required background information for effective operations and the counterpart AC operational area may both require a high level clearance for access.

  - RC members must follow intelligence oversight regulations, and be cautioned about how to exactly portray and execute their involvement in IO missions when working in the unclassified open source arena.

  - Significant policy and legal review must take place prior to assigning personnel tasks, which may face serious regulatory or legal constraints, i.e., intelligence collection. Intelligence oversight policy may not fully or clearly cover collection of information on the Internet. There are also other regulations concerning identification as a member of the military and the intelligence community that must be understood and observed.

  - Force protection issues must be addressed for any RC member tasked to explore the Internet. There is the possibility of identification of the RC member and possible retribution (e.g., malicious virus, identity theft, physical violence, etc.) for their activity on the Internet. A RC member's status under LOAC must be explored and defined. Use of the Open Source Information System (OSIS) offers a level of protection and identification as a government entity.

  - Virtual operations may require access by individuals to a range of military and government facilities with various levels of security and various systems for authorizing access. RC members, operating independently and requiring access to highly classified information, would benefit from some type of national access badge or a national clearance register. This would potentially allow them to use the facility most convenient to them when they can or need to perform their support mission. They would also benefit from a policy to quickly (or permanently) gain system access to required information systems at these

facilities. This would also benefit all the communications, intelligence and IO communities, both AC and RC.

5. **Field Observation Recommendations:**
(Note: Final LRP recommendations are at paragraph X below.)

- **Structure:**

  - A full-time support Reserve Liaison or Reserve Forces Advisor office should be created and staffed as the initial step in creation of a JRVIO organization at activities not previously having a RC support element. This element should contain individuals knowledgeable in RC administration and policies in each Service involved, should contain the AC focal point for operational coordination and should contain a civilian RC program coordinator to ensure program continuity.

  - Service policies and joint manning policies should be analyzed, and revised where necessary, to allow maximum flexibility in attracting and using personnel whose skill sets are required but who cannot be accessed because of existing military skill code mismatches or filled billets. National visibility of JRVIO billets should be considered.

- **Administration:**

  - Service policies should be analyzed and revised where necessary to allow maximum flexibility in drill scheduling and accounting. Policies should however recognize the need for and mandate periodic drill periods by RC members at an AC or RC facility to accomplish required administrative and training tasks that cannot be accomplished virtually.

- **Operations:**

  - Collaborative workspace technology allowing both synchronous and asynchronous connectivity should be identified and funded as a key enabler for any JRVIO organization to allow real time collaboration between RC members within a JRVIO element and between RC members and AC members for both operational and administrative functions. Configuration control should be exercised to enable collaboration among all JRVIO elements and all AC IO elements.

  - AC IO elements with JRVIO support should ensure that their budgeting process incorporates additional manday funding to permit use of RC support for contingency or surge events.

  - For tools development/testing, and IO exercise play, a closed loop IO network laboratory should be established for JRVIO elements and Joint commands conducting IO activities to prevent damage to active networks.

- **Resources:**

  - Further study should be done by DOD to determine policies governing involvement of ROTC and academic organizations in JRVIO tasking or Joint command IO support.

- Staffing and scheduling of JRIC sites should be examined and modified where necessary to allow maximum, flexible access to facilities and systems by JRVIO elements. (Note: Joint Reserve Intelligence Program Information Assurance PBD 707, dated December 22, 1999, will be leveraged to provide IA support at eight sites in FY01 and FY02).

- Funding for additional active duty mandays should be made available to accommodate coordination and planning for virtual operations. This will also enable the RC JRVIOs to rapidly respond to increases in requirements generated by the AC during times of increased OPTEMPO.

- **Technology and Equipment:**

  - A team with representation from DISA, DIA, and NSA should be constituted with the skills and authority to effect all required elements of connectivity between remote USG, AC or RC sites used by JRVIO personnel and their supported AC command.

  - Feasibility of a dedicated "closed loop" information systems laboratory should be investigated for use in IO exercises and for IO tool analysis and development.

  - Policies on virtual drilling and telecommuting should be analyzed and revised where necessary to account for the use of personally owned equipment for JRVIO tasks.

- **Security:**

  - The OSIS system, managed by the Community Open Source Program Office (COSPO), should be used as a primary force protection measure for all RC members communicating from non-government facilities or performing authorized tasks on non-government networks.

  - OASD/C3I should determine the feasibility for creating a national access roster, for RC members of JRVIO organizations, to permit both facility and system access for classified information at all USG, AC or RC sites designated for use by JRVIO elements. This national classified information access system would apply to all disciplines that routinely require access to highly classified information, both AC and RC.

  - Policy development for RC involvement in the IO arena must be accelerated by the Services, especially the legal aspects of Intelligence Oversight and virtual operations, to include the RC member's home or civilian workplace.

E. **Interviews with Supported Staff Representatives:** During the course of the LRP, numerous interviews were conducted with USSPACECOM (JIOC and JTF-CND), DISA, NSA, and IOTC staff members to assess their respective views of, and plans for, virtual RC IO support. These interviews culminated in the development of the individual JRVIO supporting CONOPS drafted by the organizations and included at Annex A-1. **(**Note: All resourcing issues concerned with JRVIO support to JTF-CND, by prior agreement between USSPACECOM and DISA, are covered in the DISA CONOPS.).

V. **JRVIO REQUIREMENTS DEVELOPMENT PROCESS:** As discussed in the Study Assumptions (Para. III), the identification of strategic and operational joint IO activities assessed to be appropriate and executable by the RC, capable of being accomplished virtually, and possessing a clear value to a joint customer was crucial to the successful completion of the LRP and the development of a viable JRVIO. Once the requirements and activities were developed, the issues surrounding the organizational structure, skill sets needed, personnel mix (grades and Service) and end strength totals could be addressed. Once these issues were settled, the questions of resourcing and technology needed to form a JRVIO could be assessed with greater accuracy. For this reason, the input from the first LRP Workshop was essential. The potential JRVIO joint customers and other workshop participants identified the following offensive IO (IO-O) activities as meeting the JRVIO acceptability criteria outlined above: PSYOP, EW, military deception, OPSEC, and intelligence support to IO-O. The following defensive IO (IO-D) and related activities were identified: vulnerability assessment, red teaming, IAVA compliance,
CND, incident response, website review, COMSEC monitoring, OPSEC, civil affairs, public affairs and intelligence support to IO-D. The following IO-O and IO-D activities, due to the requirement for on-site participation, training and operations, were assessed as poor candidates for RC virtual support to IO activities: physical destruction, physical security, counter-deception, counter-propaganda, CI, CNA and electronic protection.

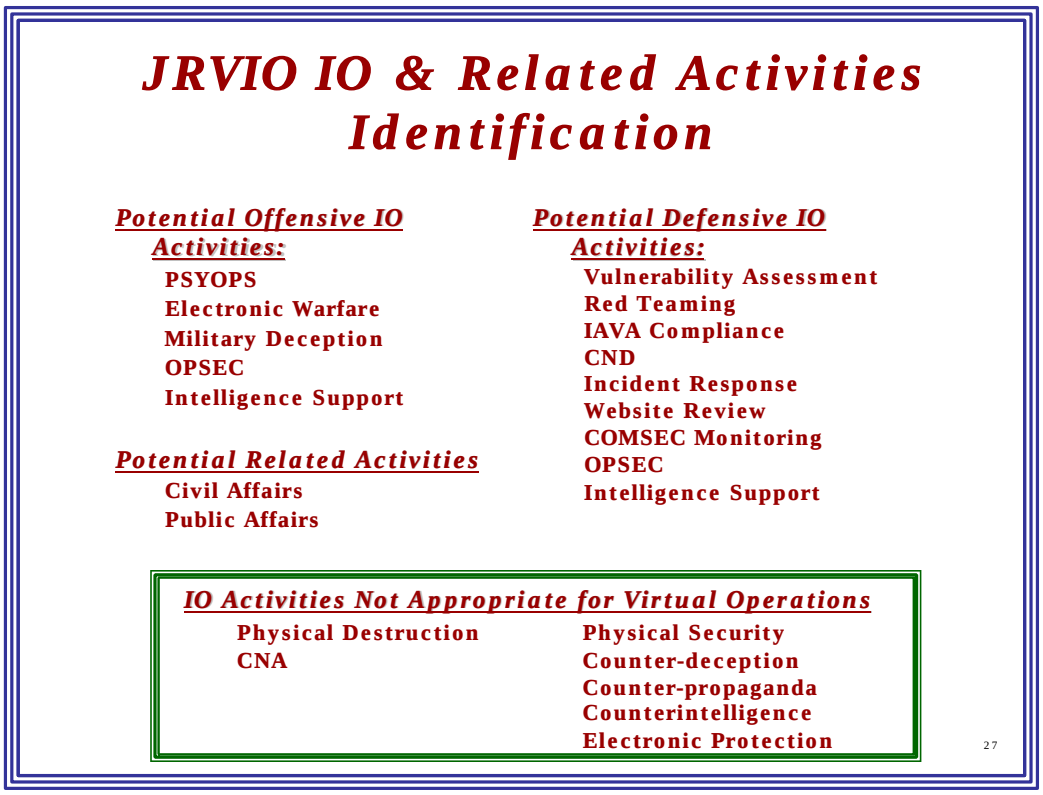

Figure 1 - JRVIO IO and Related Activities Identification

A. **Detailed Assessment of Potential JRVIO IO Activities:** Within the context of the discussion above, specific IO activities, as identified in Figure 1, were validated as appropriate for JRVIO execution by the joint IO organizations identified above.

B. **JRVIO IO Activities:** Figure 2, below, serves as a reference point for all discussions of JRVIO IO activities and joint participants catalogued by IO activity. At the most general level and by definition, any JRVIO organization will be involved in the conduct of IO as defined by Joint Publication 3-13, *Information Operations*. It must be clearly recognized that IO by definition is a synchronizing and integrating strategy (i.e. not a separate mission). It is a strategy that seeks to integrate and synchronize both traditional capabilities (e.g., PSYOP/counter-propaganda, deception/counter-deception, EW, etc.), and newly developed disciplines (e.g., IA, CND, etc.). Like most strategies there are both planning and execution components. The planning component involves the use of a relatively small number of skilled IO and IO-discipline specific professionals to plan, synchronize and integrate the use of the operational capabilities. The execution component involves the direct ownership and manipulation of operational capabilities. Development of memorandums of understanding (MOU) between respective Services and the Joint command is recommended to establish IO activity priorities. Additionally, several major joint intelligence organizations, the National Security Agency (NSA), the Defense Intelligence Agency (DIA), and the NORAD-USSPACECOM J-2, play critical roles in the production of intelligence to enable IO. Figure 2, in consonance with Joint Pub 3-13, depicts the two major IO subdivisions: defensive IO and offensive IO, along with the enabling support that intelligence provides. Thus, at the joint level, the appropriate IO activities are:

1. IO planning, synchronization and integration support
2. IA
3. CND
4. Intelligence support to IO

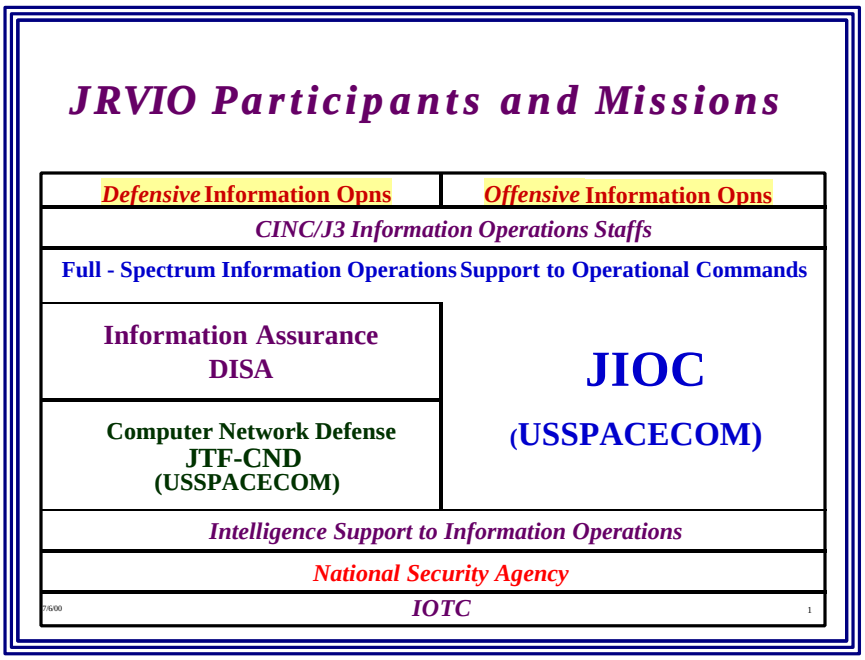

Figure 2 – JRVIO Participants and Missions

C. **JRVIO Participants (as approved in the ILRP):**[6]

1. **USSPACECOM:**

- **Joint Information Operations Center (JIOC):** On October 1, 1999, the JIOC became a subordinate activity of USSPACECOM providing full-spectrum IO support to the Unified Commands. For the most part this involves IO planning and staff assistance to CINC staffs. It should be noted that prior to October 1, 1999 the JIOC (at that time the Joint Command and Control Warfare Center) had only a Command and Control Warfare (C2W) mission. The extension of the mission to full-Service IO support came without any additional resources.

- **JTF-CND:** On October 1, 1999, the JTF-CND was reorganized under USSPACECOM to integrate and synchronize cross DOD CND operations and to provide early warning of possible network attacks. JTF-CND is not a large-scale owner of operational assets, but is instead organized as a small joint staff to execute its planning, synchronization and early warning functions. Organized as a Joint Task Force, it does have standing Service components that own the operational assets to respond to the warnings and alerts put out by JTF-CND.

2. **DISA:** At the joint level, DISA conducts IA operations to protect the Defense Information Infrastructure (DII), while the Defense-wide Information Assurance Program (DIAP) Office, DASD(S&IO)/I&IA/DIAP, has formal IA oversight responsibility for DOD. IA activities are executed through the DISA Global Network Operations and Security Center (GNOSC), the Regional Network Operations and Security Centers (RNOSCs), the DOD Computer Emergency Response Team (DOD CERT), coordination with Services and other DOD agencies, coordination with civilian industry, and a number of other internal DISA elements and external contacts.

3. **National Security Agency (NSA):** The NSA Information Assurance Directorate, in coordination with DISA, and under the policy guidance of ASD/C3I, conducts IA operations in support of both DOD and other governmental departments and agencies. NSA, like DISA, owns significant IA operational capabilities because of its mission to conduct full-spectrum IA operations.

4. **Information Operations Technology Center (IOTC):** The IOTC is a joint DOD-Director of Central Intelligence (DCI) organization housed at NSA but staffed with CNO/IT experts from across the government. The IOTC develops and brokers IO

[6] During the course of this study both the Defense Intelligence Agency (DIA) and the DOD Computer Forensics Laboratory (DCFL) evidenced an interest in developing dedicated RC IO support. Follow-on guidance to developing CONOPS and JTMD submissions may be appropriate.

technology in support of the defense and intelligence communities. Current RC support of the IOTC is provided by personnel in NSA billets on loan to the IOTC.

5. **CINC IO Staffs:** As described in Joint Pub 3-13, each Unified Commander is required to integrate capabilities to conduct IO into the command's deliberate and crisis action planning and to develop a process within the command and subordinate joint force staffs to ensure the effective integration of the various disciplines of IO in this effort. This function is normally performed by an IO staff element or cell formed from existing staff resources, and manned on an ad hoc basis, as required. Full time members of the CINC's IO Staff are augmented by individuals assigned to the functional J-codes within the staff. The issue of RC IO support to Unified Commanders will be more fully developed in the following paragraph.

D. **RC IO Support to Unified Commands:** As a part of the JRVIO study, the co-leads initiated an assessment of the current level of on-site and virtual RC IO support provided to Unified Commands. Additionally, this assessment sought to understand the reinforcing support provided to the Unified Commands by the other JRVIO participants (i.e., JIOC, JTF-CND, DISA, NSA and IOTC).

1. **Request for Information**: Data gathering was done via message to the Unified commands from the JS J1 and J3. The message solicited input from the CINCs on:

- Structure and composition of their respective IO support staffs
- RC IO support provided by organic RC support element
- The scope of current virtual RC IO support
- Assessment of current IO support provided by the JIOC

Additionally, the J3 JRVIO study co-lead followed up with the IO staff officers of the various CINC staffs during the Worldwide IO Conference in April. In the course of discussions during the Worldwide IO Conference, it was noted that the CINC IO staff officers are largely focused on skill sets supporting offensive IO as opposed to a balanced focus on both offensive and defensive IO. This led the study co-leads to conclude that the CINC message should have directly polled the J6's as well as the J1's and J3's. However, a careful review of the CINC message responses demonstrated that five of the eight CINCs responding did include data from the J6.

2. **Level of RC Support at Unified Commands:**

Unified Commands	Total RC Billets (Filled & Unfilled)[7]	RC IO Billets (Filled & Unfilled)[8]	RC IO Virtual Support[9]
USEUCOM	1016	See Below[10]	See Below[11]
USPACOM	1917	5	See Below[12]
USCENTCOM	754	7	Yes[13]
USSOUTHCOM	426	0	No
USSOCOM	490	0	No
USJFCOM	1505	25	No
USSPACECOM&	453	17	No
USSTRATCOM	326	0	No
USTRANSCOM	193	0	No
Total	**7080**	**54**	

Table 1

3. **Virtual IO Activities at Unified Commands:**

- **Current Extent of Virtual Operations:** Three of the eight Unified Commands responding to the request for information noted current use of virtual operations in execution of IO activities. USEUCOM stated that they receive significant virtual IO/IA support from JS J39, JIOC, IOTC and JWAC. They were not aware if the RC was involved in providing any of this support. USEUCOM enthusiastically endorses more extensive use of virtual modalities, especially as they involve the RC. USPACOM noted that formal reachback (teleconference, computer link) to the JIOC exists, but the level is insignificant and the change in the workload of the USPACOM IO staff is negligible. USCENTCOM noted a more extensive use of virtual operations. According to the USCENTCOM response, reach-back and virtual support to planning and the conduct of current operations is critical and ongoing. For example, the 4th PSYOP Group, 8th PSYOP Battalion, Ft. Bragg, NC, supports a

[7] Each CINC associated entry in this column represents the total number of RC billets on the associated JTMD both funded and unfunded across all J-codes.
[8] This column does not include intelligence support to IO for reasons stated below in footnote immediately following. Also the numbers in this column only reflect RC IO billets on CINC HQ staffs.
[9] The majority of the Unified Commands receive virtual RC intelligence support, a portion of which may be directly linked to enabling IO activities. However, for the purposes of this table, intelligence support to IO is not considered as an IO capability. This approach is consistent with Joint Doctrine, which regards intelligence as an IO enabler but not an IO capability.
[10] USEUCOM stated IO staff support is provided by members of their joint staff on a matrixed basis. They believe that at full mobilization there would be significant RC presence on the RC IO staff, but this number cannot be captured at this time.
[11] USEUCOM states that they receive significant virtual IO support from JIOC, IOTC, Joint Warfare Analysis Center (JWAC) and JS J39. They are not aware if any of that support is being provided by RC members. USEUCOM strongly supports the use of virtual support and a study of how the RC can best be used to provide IO/IA virtual support.
[12] USPACOM stated that they have received virtual IO support from the JIOC. They did not know if the JIOC was using any RC personnel to provide this support. It should also be noted that USPACOM does receive virtual RC intelligence support, a portion of which may be IO/IA related.
[13] USCENTCOM stated that they made extensive use of virtual RC IO capabilities resident in Army PSYOP organizations. However, this was not a number that they felt could be easily quantified.

myriad of USCENTCOM IO efforts in the AOR. Depending on the nature of the USCENTCOM effort, additional support can and has been garnered via telephonic conferencing and VTC from agencies ranging from DIA to the JWAC. The USCENTCOM response went on to state that with mention of the 4th POG above, depending on the size of the operation, RC augmentation is a critical piece to mission accomplishment and has been utilized with great success. RC support to USCENTCOM through virtual means has been excellent (completely transparent) to date. Additionally, it was noted that USSOCOM while not currently conducting any virtual IO activities is developing a distance learning capability to support the Special Operations Forces (SOF) IO education and training program in the mid-term. The entry-level course on SOF IO will be modularized to provide familiarization for home station and deployed SOF elements.

- **Potential Virtual IO Activities:** Unified Command IO staff officers polled at the World-Wide IO Conference felt that perhaps intelligence support could be accomplished virtually, because they only need to see the end product. As long as the intelligence is timely, accurate, and relevant, users are not concerned with who does the analysis. In addition, USPACOM noted that it is quite possible that IO functions concerning PSYOP could quite skillfully and appropriately be met by Reservists who have highly sought-after civilian employment skills developed from working at advertising agencies, TV and radio broadcast stations, and magazines and newspapers (especially those using satellite technology such as *USA Today*). With the appropriate level bandwidth, products created virtually in the audio-visual realm could easily be transmitted worldwide. Translating products into foreign languages could also be accomplished by skilled virtual linguists. A special technical operations (STO) organization could also be value-added via appropriate reachback connectivity.

- **Virtual versus On-site Support:** According to the IO staff officers polled at the World-Wide IO Conference, the geographic CINCs are more interested in on-site support than virtual support, and particularly so when crisis action and deliberate planning are the supported processes. They largely discounted the ability of the RC to provide them with virtual IO planning support as they considered it unworkable and generally too difficult to manage. USPACOM made this point very forcefully in its message response when it stated that full time, on-site RC IO support would be the most helpful. However, USPACOM stated that they believed that anything, to include virtual RC IO support, that had the potential to benefit them directly should be studied as long as there were no resourcing implications for their existing RC support element.

4. **IO Support Provided by the JIOC:**

- Overview: All of the Unified Commands noted that they receive IO support from the JIOC. Furthermore, all stated that the support has been an integral part of their

respective IO activities and efforts and especially so for planning and exercise support. Unified Command responses that provided significant detail regarding JIOC support are summarized below as a means of better understanding the types of support and manner in which it is provided by the JIOC.

- **USSPACECOM:** USSPACECOM stated that it has no organic IO support. USSPACECOM relies heavily on the JIOC for support during exercises, crises or contingency operations. USSPACECOM generally uses JIOC capabilities in a staff augmentation role. Part of the support that the JIOC provides to USSPACECOM is done virtually.

- **USJFCOM:** The JIOC has provided key support to the USJFCOM IO staff during joint and CINC-level exercises. Joint IO/IW subject matter experts (SMEs) from the JIOC filled joint manning document slots in USJFCOM exercises such as UNIFIED ENDEAVOR, a JTF-level training exercise series; and EVIDENT SURPRISE, a series of USJFCOM directed strategic-level IO-specific exercises. For UE-98-3/FUERTAS DEFENSAS 98-99, the JIOC CINC country team produced an extensive C2 capabilities study which combined real-world and notional data to provide a robust environment for IO planning. Additionally, JIOC planners developed IO injects for the master scenario events list. A JIOC red team SME was also integrated with the Joint Warfighting Center (JWFC) OPFOR and assisted in developing a credible OPFOR IO threat throughout the exercise. A team of JIOC technicians worked with JWFC personnel to run the "J-quad IO model" and supported both intelligence and IO-specific battle damage assessment (BDA). JIOC support to past USJFCOM exercises combined on-site representation with reachback to databases through SIPRNET and the Joint Worldwide Intelligence Communications Systems (JWICS).

- **USPACOM:** USPACOM noted that the JIOC was actively trying to improve its support to USPACOM. Most of the JIOC's support to USPACOM is in Tier 1 and Tier 2 exercise development and execution. JIOC support during Tier 1 exercises consisted of augmenting the IO Strategy Cell, the Joint Exercise Control Group, and the After Action Review Group during the major joint exercise, ULCHI FOCUS LENS (UFL) in August 99. They augmented again during the reception, staging and onward integration (RSOI) exercise in April 00 and UFL in August 00. Without JIOC augmentation for Tier 1 exercises, USPACOM J39 would not be able to implement full-spectrum IO during these exercises. JIOC support was also used during the East Timor crisis and execution when they augmented USPACOM's IO planning cell to help develop IO planning documents. To ensure the best use of a limited resource, USPACOM J39, in coordination with JIOC, is attempting to prioritize the many requirements for JIOC assistance that come from within the theater. The JIOC has also reviewed IO appendices and other deliberate planning efforts, but not enough to consider it as a true reachback capability in USPACOM's

eyes. However, USPACOM noted the JIOC's PSYOP specialist was very active in IO appendix development for a major theater plan. Finally, USPACOM noted that on occasion, it has used classified computer systems to send draft IO appendices to JIOC for review and that while deployed, JIOC personnel have used this reachback capability to access information to assist in the development of IO campaign plans. According to USPACOM, the reachback capability was a useful tool but not a critical one.

- **USEUCOM:** USEUCOM stated that they receive significant support from the JIOC but that experience has taught them that they need an increase in the size of the JIOC CINC Support Team dedicated to USEUCOM. Further, USEUCOM stated that they believed that OPSEC and deception support capabilities should be added or increased within their CINC Support Team.

5. **Overall Assessment:** It is the opinion of the JRVIO study co-leads that the Unified Command IO staff officers do not fully understand the JRVIO concept, RC IO/IA capabilities, or the implications of virtual operations. It is believed that the JS J1/J3 message did cause the Unified Commands to examine how their RC support elements were currently being used and whether or not a realignment to weight support towards IO was appropriate. It is apparent that the increased RC support to Unified Command IO staffs would immediately improve the effectiveness and synergy of Unified Command IO activities. What is not known is how much of that support could be accomplished virtually. The study co-leads determined that a major study recommendation would be to follow up with the Unified Commands with regard to the RC IO support and the potential to augment existing Unified Command IO staffs with JRVIO support.

VI. **JRVIO IMPLEMENTATION STEERING GROUP:** A JRVIO Steering Group (JSG) will be established to oversee the JRVIO LRP implementation.

A. **Development:** The ASD/RA, ASD/C3I and JS Directors of J1, J3 and J6 will report back within 45 days of final report approval with a recommendation on the JSG's organization and charter.

B. **Representation:** At a minimum JSG representation will include OASD/C3I, OASD/RA, JS, USSPACECOM, NSA, DISA, IOTC, the Services, the RCs and any other DOD element deemed necessary by the JSG leadership.

C. **Follow-on Issues:** The JSG has oversight of JRVIO follow-on issues as described in this report and has the authority to delegate responsibilities and tasks as required. In this case, oversight is defined as monitoring the progress of the follow-on actions cited in this report and providing advice to the authorities responsible for implementation and policy development. As a minimum, the JSG will maintain oversight of the following JRVIO issues:

1. Refinement of the JRVIO CONOPS activities

2. Enabling JRVIO technologies and equipment

3. JRVIO support to the Unified Commands

4. Joint command submission of JRVIO manpower requirements

5. Training strategy for JRVIO personnel using model at Annex A-2

6. Personnel management issues approved in the ILRP and listed in paragraph VIII below

D. **Sub-committees:** The JSG is authorized to establish sub-committees to monitor follow-on issues and make appropriate recommendations.

E. **Reporting:** The JSG will update the DEPSECDEF annually through FY 04 on JRVIO implementation.

VII. JRVIO CONCEPT OF OPERATIONS:

A. **Background:** DEPSECDEF approval of the JRVIO CONOPs will not create new kinds of DOD organizations. JRVIO will be built out of the well-established JTMD staffing process and result in the stand-up or augmentation of RC support units. In approving the JRVIO ILRP, the DEPSECDEF directed the use of an operational concept model for the phased creation of multiple, small, independent JRVIOs under the control of the supported organization. The DEPSECDEF further approved creation of JRVIOs in support of four major players: NSA, IOTC, DISA, and USSPACECOM (JIOC and JTF-CND). As depicted in Figure 3 below, the approach approved by the DEPSECDEF achieves the objective organizational end state of multiple, small, independent JRVIOs structured to the supported joint organizations. Further, this approach provides for dedicated, direct support, and achieves the objective operational end state via the phasing of operational capabilities. It envisions achieving near-term JRVIO operational capability via a “mandays solution” using Reserve Personnel Special Training funds. Longer term “organizational ownership” of all required JRVIO JTMD spaces by supported joint organizations mentioned in this report would be achieved by submission of required documents into the Joint Manpower Program staffing and the Planning, Programming, Budget System (PPBS) processes.

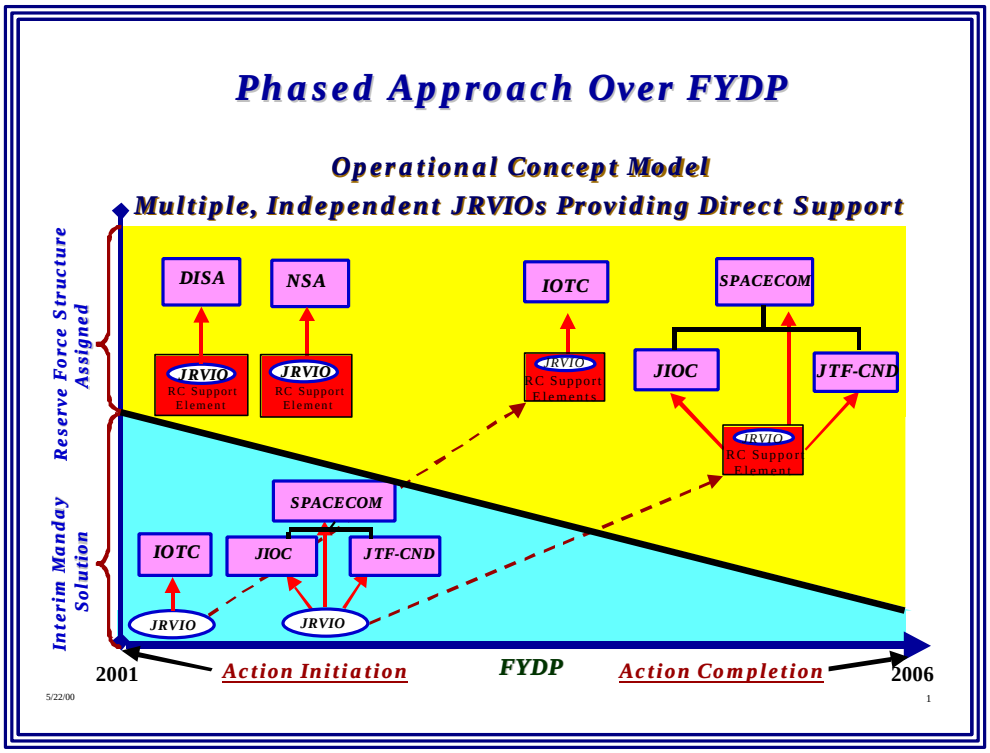

Figure 3 – JRVIO Operational Concept Approved by DEPSECDEF

B. **Structure and Functions:** The structure and functions of each JRVIO mirror that of the AC (e.g. the JRVIO supporting the JIOC will execute functions within the scope of the JIOC's mission). There is no function, other than conducting virtual operations, the JRVIO will undertake that varies from the missions assigned to its supported unit. The structure of the JRVIOs is common to many other RC elements supporting various DOD organizations. FTS are limited to administration and coordination of JRVIO operational activities, while mission execution will be conducted by traditional RC personnel. In aggregate, all six DOD RCs will take part in the JRVIO effort.

C. **Command and Control Relationships:** The command and control (C2) relationships internal and external to the multiple JRVIOs are consistent with those of other, non-virtual RC units. C2 will be exercised as in any existing RC chain of command. The supported organization will assign missions to the supporting organization for their primary peacetime missions. Upon mobilization, operational control (OPCON) will be exercised by the commander designated to receive OPCON by the SECDEF or, when authorized, by the appropriate combatant commander. The JRVIOs will rely on dedicated FTS personnel resident at the supported organization in an existing or planned RC support element.[14] These FTS personnel along with parent RC Commanders will provide administrative support and operational coordination in accordance with Service procedures and pre-existing arrangements (Administrative control will be exercised through approved Service channels

[14] DISA and NSA have existing RC support elements, whereas the JIOC and IOTC plan to establish RC support elements in the near future.

and in accordance with established Service procedures. This situation is analogous to the contemporary management of Unified Command and Combat Support Agency RC support elements.). (Note: The requirement for dedicated FTS to enable JRVIO organizations was a key lesson learned from the proof of concept.) Mission and administrative guidance will flow from the various staff elements designated by the supported organizations for JRVIO support to the virtual organization. In terms of administrative guidance, the full time personnel supporting the JRVIO at each organization will provide administrative support, managerial direction and operational focus. They will work to identify and access appropriate JRVIO personnel and to enable JRVIO operations at minimal cost to the supported organization via utilization of existing AC and RC systems, equipment and facilities infrastructure. The parent RC will provide administrative support for Service specific matters. Some training for JRVIO members may be required on-site. However, under routine operational conditions, the normal mode of operation for the JRVIOs will be to accomplish required training, administration and assigned missions, tasks and activities virtually.

D. **Resources:** The following was developed through multiple workshops and face-to-face discussions with staff elements from USSPACECOM (JIOC & JTF-CND), DISA, NSA and IOTC. (Note: JRVIO support to JTF-CND, by prior arrangement between DISA and USSPACECOM, will be provided by DISA.)

1. **Manpower:**

- **JRVIO Data Distribution:** Each of the major JRVIO participants is addressed in its own subparagraph below. Tables 2, 3, 4, and 5 provide contextual data displaying: the size of each organization's overall RC support element; the percentage of support currently dedicated to IO/IA on-site and virtual activities; the additional RC billets each organization will be requesting to conduct IO/IA activities; and, the percentage of "to be requested" RC IO/IA strength that will conduct virtual operations. Table 6 provides a consolidated look at each participants new JRVIO associated requirements (Note: Table 6 does not include DISA and NSA personnel already on hand that meet JRVIO criteria. Table 6 only includes JRVIO associated new requirements.). It should be noted that the data provided below is directly supported by the JRVIO supporting CONOPS at Annex A-1. Finally, Table 7 provides a cumulative look at both JRVIO manpower and funding requirements.[15]

- **JRVIO RC Personnel Mix:** While the JRVIO Tables that follow reflect requirements by Service, the actual distribution of JRVIO associated billets will be determined as a result of consultations between the Services and JS during the individual JTMD staffing processes. The Service related requirements reflected below represent numbers provided by JRVIO participants in their supporting CONOPS (See Annex A-1).

[15] While tables below do not reflect RC support by unit organization, Services will determine appropriate individual vs. unit mix.

- **Joint Information Operations Center Contextual Data[16]:**

RC Support By Type	Current RC Support	% of RC Supporting IO/IA Activities	% of RC IO/IA Support Operating Virtually	New RC IO/IA Billets From Upcoming JTMD/POM	% of New RC IO/IA Billets Operating Virtually[17]
Full Time:					
Air Force					
Officer				2	
Enlisted				0	
Army					
Officer				1	
Enlisted				0	
Navy					
Officer				1	
Enlisted				0	
Marine Corps					
Officer				0	
Enlisted				1	
Total – Full Time				**5**	
SELRES:					
Air Force					
Officer				39	
Enlisted				15	
Army					
Officer				29	
Enlisted				16	
Navy					
Officer				39	
Enlisted				11	
Marine Corps					
Officer				11	
Enlisted				2	
Total - SELRES				**162**	
TOTAL				**167**	**89% (149)**

Table 2

[16] JIOC currently has no RC support and therefore the first three columns are left blank.

[17] For purposes of this study, all FTS dedicated to enabling virtual operations are considered as an integral part of the JRVIO regardless of location.

- **National Security Agency Contextual Data[18]:**

RC Support By Type	Current RC Support	% of RC Supporting IO/IA Activities	% of RC IO/IA Support Operating Virtually	New RC IO/IA Billets From Upcoming JTMD/POM	% of New RC IO/IA Billets Operating Virtually
Full Time:					
Air Force					
Officer	2			1	
Enlisted	1			0	
Army					
Officer	2			1	
Enlisted	0			0	
Navy					
Officer	1			0	
Enlisted	0			1	
Marine Corps					
Officer	0			0	
Enlisted	0			0	
Total – Full Time	**6**			**3**	
SELRES:					
Air Force					
Officer	80			6	
Enlisted	237			31	
Army					
Officer	15			8	
Enlisted	35			18	
Navy[19]					
Officer	180			11	
Enlisted	540			56	
Marine Corps					
Officer	15			6	
Enlisted	30			11	
Total -SELRES	**1132**			**147**	
TOTAL	**1138**	**11% (125)**	**23% (29)**	**150**	**100% (150)**

Table 3

[18] Joint Publication 3-13 views intelligence as an integral part of IO and is a fundamental enabler of all IO/IA activities. However, at the request of NSA, for this study the RC support to IO at NSA will be confined to that support provided by the RC to either X-Group, the Defensive Information Operations Organization, or IOTC.

[19] Navy totals include all Naval Reserve Security Group (NRSG) manpower. Double counting of NRSG assets by other agencies is possible under the JRVIO study. Currently, most NRSG billets and NSA support personnel are involved in SIGINT, not INFOSEC.

- **Information Operations Technical Center Contextual Data[20]:**

RC Support By Type	Current RC Support	% of RC Supporting IO/IA Activities	% of RC IO/IA Support Operating Virtually	New RC IO/IA Billets From Upcoming JTMD/POM	% of New RC IO/IA Billets Operating Virtually
Full Time:					
Air Force					
Officer				1	
Enlisted				1	
Army					
Officer				1	
Enlisted				0	
Navy					
Officer				0	
Enlisted				1	
Total - Full Time				**4**	
SELRES:					
Air Force					
Officer				20	
Enlisted				12	
Army					
Officer				20	
Enlisted				12	
Navy					
Officer				12	
Enlisted				12	
Marine Corps					
Officer				8	
Enlisted				4	
Total - SELRES				**100**	
TOTAL				**104**	**50%(52)**

Table 4

[20] IOTC has no RC support element; IOTC does have some RC staffing borrowed from the NSA RC account.

- **Defense Information Systems Agency Contextual Data[21]:**

DISA RC Support By Type	DISA Current RC Support	% of RC Supporting IO/IA Activities	% of RC IO/IA Support Operating Virtually	New RC IO/IA Billets From Upcoming JTMD/POM[22]	% of New RC IO/IA Billets Operating Virtually
Full Time:					
Air Force					
Officer	1			2	
Enlisted	0			10	
Army					
Officer	0			0	
Enlisted	0			0	
Navy					
Officer	0			0	
Enlisted	1			0	
Marine Corps					
Officer	0			0	
Enlisted	0			0	
Total – Full Time	**2**			**12**	
SELRES:					
Air Force					
Officer	55			69	
Enlisted	23			244	
Army					
Officer	15			52	
Enlisted	121			49	
Navy					
Officer	3			13	
Enlisted	16			10	
Marine Corps					
Officer	7			9	
Enlisted	5			24	
Total - SELRES	**245**			**470**	
TOTAL	**247**	**70% (173)**	**85% (147)**	**482**	**58.5% (282)**

Table 5

[21] All resourcing issues concerned with JRVIO support to JTF-CND, by prior agreement between USSPACECOM and DISA, are included in the DISA data.
[22] Documentation requesting all displayed increases to DISA JTMD was forwarded to JS in April 2000.

- **Combined JRVIO Manpower Requirements**[23]**:**

FTS:	JIOC	NSA	IOTC	DISA	Totals
Air Force					
Officer	2	1	1	0	4
Enlisted	0	0	0	10	10
Army					
Officer	1	1	0	0	2
Enlisted	0	0	0	0	0
Navy					
Officer	1	0	0	0	1
Enlisted	0	1	1	0	2
Marine Corps					
Officer	0	0	0	0	0
Enlisted	1	0	0	0	1
Total - Full Time	**5**	**3**	**2**	**10**	**20**
SELRES:					
Air Force					
Officer	35	6	10	46	97
Enlisted	13	31	6	147	197
Army					
Officer	26	8	10	31	75
Enlisted	14	18	6	29	67
Navy					
Officer	35	11	6	8	60
Enlisted	10	56	6	6	78
Marine Corps					
Officer	9	6	4	5	24
Enlisted	2	11	2	0	15
Total - SELRES	**144**	**147**	**50**	**272**	**613**
TOTAL	**149**	**150**	**52**	**282**	**633**

Table 6

2. **Facilities and Equipment:** Equipment and facilities synergy will be gained by making extensive use of existing infrastructure. The multiple JRVIOs will train and operate in facilities and with hardware and software that are already contained within established AC, RC, governmental and private facilities capable of hosting JRVIO

[23] It should be noted that Table 6 does not include on hand personnel in DISA or NSA that already meet JRVIO criteria. Instead, the exclusive focus is on the JRVIO associated new requirements.

personnel. Both DISA and NSA have extensive infrastructure in place. In addition, the JRICP program provides connectivity at (28) RC sites nationwide. By maximizing availability of these assets during the periods when RC members are usually available (evenings and weekends), the need for additional facilities and equipment will be minimized. Minimal O&M funding is included in this proposal for JRVIO specific infrastructure changes. Resourcing synergy will be gained by leveraging the infrastructure and connectivity capabilities to be made available as a result of the Joint Reserve Intelligence Program Information Assurance, Program Budget Decision (PBD) 707, 22 December 1999, initiatives, providing $4.9 million for FY01 in O&M funds. A possible requirement for additional equipment would be for individual Unified Command "closed loop" IO network laboratories that could be used for IO exercises and also be used for tool assessment. It will be the responsibility of the supported and supporting organizations to project and fund for additional infrastructure requirements.

3. **Funding:**

- **Overview:** JRVIO is a new, unfinanced requirement. It is assumed that out-year RC manpower end strength for drilling personnel will remain constant. Resourcing for new JRVIO billets will require realigning current RC manpower from other existing joint or Service assets. Manpower above current end strength would be required for full-time support. For the Future Years Defense Program (FYDP), and due to the (PPBS) cycle, any manpower resourcing prior to FY03 will have to use existing resources through realigning manpower or realignment of RC Special Training (ADT/ADSW) manday support within individual RCs, or through a combination of both.[24]

  - ✔ The main thrust of the JRVIO resourcing strategy is to provide all FY01 and FY 02 RC support for JRVIO through manday support and to transition to funded RC JRVIO billets during FY03 to FY07. Active duty manday funding is therefore required in the near term so that joint IO commands may receive RC support from other Service/RC IO commands as they attempt to meet current commitments and to initiate virtual IO/IA support operations prior to the allocation of dedicated JRVIO manpower authorizations.

  - ✔ **Funding Management and Distribution:**

    - ♦ **Personnel:** Requirements for JRVIO personnel funds will be coordinated with OASD/RA to determine Service distributions. Personnel funds comprise the bulk of requested JRVIO funding and are used to offset manpower and manday costs.

    - ♦ **O&M:** JRVIO operations and maintenance funds will be distributed in coordination with OCJCS, OASD/C3I and OASD/RA to the Services to support their RC's JRVIO operations and maintenance. O&M funds provided

[24] While it is not clear that there are any unique universal JRVIO training requirements, should some be identified, O&M funds may be used to compensate Services for required training.

under the Joint Reserve Intelligence Program Information Assurance, PBD 707, for operating costs will be administered by USJFCOM.

♦ **PBD 707:** Further resourcing synergy will be gained by leveraging the infrastructure and connectivity capabilities provided for in the Joint Reserve Intelligence Program Information Assurance Program Budget Decision (PBD) 707, 22 December 1999.

4. **Estimated Manpower and Funding Table:**

JRVIO Supported Organization		**FY01**	**FY02**	**FY03**	**FY04**	**FY05**	**FY06**	**FY07**
JIOC								
Officer		**11**	**11**	**30**	**49**	**68**	**87**	**105**
Enlisted		**4**	**4**	**11**	**18**	**25**	**32**	**39**
NSA								
Officer		**6**	**6**	**11**	**16**	**21**	**26**	**31**
Enlisted		**16**	**16**	**36**	**56**	**76**	**96**	**116**
IOTC								
Officer		**3**	**3**	**9**	**15**	**21**	**27**	**30**
Enlisted		**2**	**2**	**6**	**10**	**14**	**18**	**20**
DISA (& JTF-CND)								
Officer		**40**	**40**	**90**	**90**	**90**	**90**	**90**
Enlisted		**100**	**100**	**182**	**182**	**182**	**182**	**182**
Total RC Manpower								
Officer		**60**	**60**	**140**	**170**	**200**	**230**	**256**
Enlisted		**122**	**122**	**235**	**266**	**297**	**328**	**357**
Estimated Manday $		**$2.064M**	**$2.140M**	**$1.000M**	**$875K**	**$625K**	**$500K**	**$500K**
Estimated RC Billet $[25]		**$0**	**$0**	**$3.700M**	**$4.830M**	**$6.145M**	**$7.397M**	**$8.487M**
FTS Manpower								
Officer		**0**	**0**	**3**	**4**	**5**	**6**	**7**
Enlisted		**0**	**0**	**6**	**8**	**10**	**12**	**13**
Total FTS $		**$0**	**$0**	**$663K**	**$913K**	**$1.178M**	**$1.459M**	**$1.692M**
O&M $		**$0**	**$393K**	**$563K**	**$639K**	**$715K**	**$791K**	**$831K**
Total $		**$2.064M**	**$2.533M**	**$5.926M**	**$7.257M**	**$8.663M**	**$10.147M**	**$11.510M**

Table 7

[25] RC personnel required to establish JRVIO units will be programmed by the Services from existing end strength resources in FY 03 and the out years.

5. **Resourcing Recommendation:** DEPSECDEF consider additional active duty manday funding in the Service active military personnel appropriations for JRVIO implementation in FY01 ($2.064 million) and FY02 ($2.533 million) during the FY 02 Budget Review. These funds would allow Joint IO commands to receive RC support from other Service/RC IO commands as they attempt to meet current commitments and to initiate virtual IO/IA support operations prior to the allocation of dedicated JRVIO manpower authorizations. Additionally, DEPSECDEF approve additional FTS personnel for JRVIO units as the concept and requirements of the mission mature in the FY 03 Program Review or Budget Review process. Per Table 7, funding requirements would range from $663 thousand in FY 03 to $1.692 million in FY 07.

E. **Security:** Depending on the mission, it is envisioned that JRVIO personnel may require up to a Top Secret/Sensitive Compartmented Information (TS/SCI) clearance. While it is recognized that some or most of the missions may be conducted in an unclassified environment, a collateral or TS/SCI clearance may be necessary in order to provide the appropriate level of training or operations preparation prior to mission execution. The mere process of reading personnel into the function and nature of the supported organization's activities may necessitate a clearance.

VIII. **PERSONNEL MANAGEMENT:** The following recommendations for personnel management actions to facilitate the implementation of a JRVIO were developed in detail in the ILRP and were approved for action by the DEPSECDEF. No further personnel management issues were developed as a result of the final lessons learned from the PoC. However, minor changes were made to the telecommuting and accession and retention paragraphs. After vetting of the interim recommendations against the results of the proof of concept lessons learned/field observations, the co-leads now endorse the following as the final recommendations regarding personnel management.

A. **Military Specialty Codes:**

1. Services consider revising CNO/ IT function codes to more accurately reflect CNO/IT activities.

2. Services consider developing functional areas and special skill identifiers, to further identify CNO/IT skilled personnel.

B. **Civilian Acquired Skills:**

1. DOD continue working to select a common operational "CNO/IT skills database" that allows for the rapid retrieval of detailed information on both civilian and military acquired CNO/IT skills.

2. DOD consider developing policy guidance that mandates population of the database by all RC personnel.

3. DOD consider developing policy guidance that directs the Services to sustain the currency of the CNO/IT skills database.

4. CINCs, Services and agencies consider identifying RC manpower and personnel assigned to CNO/IT functions.

5. CINCs, Services and agencies consider entering the required CNO/IT function information into the appropriate databases.

C. **Accession and Retention:**

1. DOD consider establishing an OSD-sponsored steering group to focus on military CNO/IT personnel issues.

2. Services examine potential policies that treat selected CNO/IT sub-specialties in the same manner as medical doctors, lawyers and chaplains for waiving paygrade and age requirements while allowing direct commissioning.

3. Services examine potential for employing professional or bonus pay for accessing and retaining CNO/IT personnel into pay/drill status.

4. Services examine providing for responsive reclassification of military specialty codes based upon civilian acquired skills.

D. **Career Progression:**

1. Services consider developing the means to mitigate the “up and out” and “up or out” personnel handling procedures for high demand, CNO/IT skilled personnel.

2. Services consider developing procedures to ensure that personnel assigned to the JRVIO are promoted at a rate at least equal to that for non-JRVIO personnel serving in the same career path.

E. **Performance Monitoring:** No change to current policies is deemed necessary.

F. **Security Requirements:**

1. CINCs, Services and agencies consider reevaluating classification requirements for IO and related activities billets in the JRVIO.

2. DOD consider targeting individuals selected for an assignment within the JRVIO requiring a security clearance for priority handling of the security clearance determination and adjudication process.

3. DOD consider reviewing the current Joint Reserve Intelligence Center (JRIC) infrastructure associated security requirements in order to determine required security clearance measures needed to allow JRVIO members full utilization of the JRIC sites.

G. **Training Strategy:**

1. CINCs, Services and agencies consider establishing mandatory training and/or certification programs for CNO/IT skills and functions.

2. CINCs, Services and agencies consider fully documenting required mandatory CNO/IT training and/or certification programs.

3. CINCs, Services and agencies consider conducting mandatory periodic reviews of CNO/IT training and/or certification programs.

4. DOD consider developing an ADL program, including a certification management system, for CNO/IT training and certification.

5. RC consider allowing personnel to telecommute and use ADL and web-based training for IO/CNO/IT/skill certification and training.

6. RC consider waiving CNO/IT training requirements if personnel can certify equivalent competence based on civilian acquired skills.

H. **Flexible Drilling Policies:**

1. DOD consider issuing flexible drilling policy guidance in order to standardize Service utilization of this key JRVIO enabling process.

2. CINCs, Services and agencies consider issuing policy guidance in line with DOD flexible drilling guidance.

I. **Telecommuting Policies:**

1. DOD review current IO telecommuting and flexible drilling policy guidance to determine whether these policies should be standardized across Services, agencies and Unified Commands. These issues may include force protection, line of duty, UCMJ, intelligence oversight training/monitoring, LOAC, and time and attendance/performance monitoring.

2. CINCs, Services, agencies consider issuing policy guidance in line with DOD Telecommuting guidance.

IX. **TECHNOLOGY:** In the early stages of a JRVIO organization(s), no technology obstacles associated with the PoC conducted were noted. However, the rapid evolution of technology will provide unique solutions and some challenges to the stated end state goals.

Taking advantage of technology today is a resource constraint not a technology shortfall. One of the keys required is to ensure interoperability at all levels and maintenance of standards, both hardware and software, across the operational networks. Collaborative planning tools were identified to the field in an April 2000 JS message, with the idea to settle on one or two collaborative tools. This is key to both short and long term success in implementation of the program. The working group identified four critical technology areas warranting further research: Collaborative planning tools; public key infrastructure/multi-level security; accountability/audit software and use of virtual private networks.

A. **Collaborative Planning Tools :**

1. **Background:** Often displayed as a building with rooms, the Collaborative Workspace Environment (CWE) is an automation environment that enables people to converse, collaborate, and interact regardless of geographic location. The workspace establishes and manages a collection of virtual rooms; each incorporating the people, information, and tools appropriate to a task, operation, or service. Users can move from room to room just as we would in a building, meeting team members, discovering collaborators, sharing knowledge, and performing functions as they would if physically collocated.

2. **Discussion:** A requirement exists for an automated tool(s) that will enable preservation of critical human activity (collaboration and interaction) while establishing a standard environment for virtual team operations. This capability will allow JRVIO operations to create and manage real-time information (files, thoughts, reports, etc.) related to a common effort regardless of geographic location. The following information is pertinent:

- An OSD/C3I / JS "Tiger Team" is addressing a three-phase way-ahead strategy for DOD collaborative tools.[26] Based upon CINC/Service/Agency requirements the following systems were selected for evaluation: Collaborative Virtual Workspace (CVW), Odyssey, Information Workspace (IWS), Netmeeting (with White Pine Server and Outlook), and Sametime/Realtime (with Domino Server and Lotus Notes).

- The selected systems are currently used by the intelligence activities assigned to the JS "Tiger Team".

- The USJFCOM Joint Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) Battle Center (JBC) is running a comparative assessment for the purpose of selecting an interim standard.

- JBC will develop a staff recommendation for the DOD Chief Information Officer (CIO) Executive Board for a permanent collaborative strategy.

- Regardless of which standard is selected, initial training requirements and

[26] JCS // DJS// Electronic message dated 19 April 2000, Subject; Collaborative Tools Update (U)

certification of JRVIO will be a resource issue.

- JRVIO should limit acquisition of collaborative planning tools to one of the endorsed configurations.

- Bandwidth is a critical resource inhibitor to the use of collaborative planning tools.

- In addition to the efforts made by the JS "Tiger Team" to standardize future CWE operations, DOD currently supports a distributive virtual network in support of distance learning programs. The evolution of ADL architectures emphasizes synchronous and asynchronous collaboration on standards-based versions of reusable objects, networks, and learning management. This architecture may provide shareable resources, lessons learned, and architecture to support near and interim term JRVIO missions.

3. **Recommendations:** The JRVIO co-leads should sustain the JRVIO Technology Sub-committee to remain current on emerging capabilities that relate to JRVIO. Virtual workspace and interoperability are critical to the success of JRVIO. Initially, the Technology Sub-committee should focus on the following challenges:

- They should work closely with the "Tiger Team" to capitalize on the anticipated fielding of a standardized collaborative workspace tool.

- Acquisition of collaborative planning tools for near and intermediate term JRVIO participants must be limited to one of the five virtual capabilities listed above. This is necessary to ensure maximum interoperability within DOD architectures.

- They should evaluate ADL training and network technology for JRVIO applicability.

B. **Performance Monitoring Requirements:** The JRVIO concept raises challenges not found in a traditional work environment. The very technology that offers the freedom to work anytime and anywhere also limits the creation of shared reality and measurable work expectations. Current DOD concepts of organizational effectiveness (e.g., dress and appearance codes, training plans, maintenance records) will require modification to fit within the virtual operations world.

1. **Background:** The traditional work environment provides supervisors and consumers the ability to directly evaluate the performance and accountability of the workforce. In the virtual environment, training, team building and evaluation of individual performance will require special tools for control and coordination.

2. **Discussion:** Various software programs support an automated audit trail of online use. These programs can monitor when an individual logs onto the network, what directories were accessed, and what documents were created or used. Commercial

software ranging from server security to dedicated programs is available to provide measurable (yet undefined) performance assessments. One example reviewed by the sub-committee is Boss Everyware[27] which has the following capabilities:

- Supports "positive accountability" of members.
- Satisfies traditional audit data requirements.
- Tracks time and activities.
- Record files used, "products" created, and keystrokes.
- Appends multiple user files.
- Corporate licenses available.

3. **Recommendations:** The JRVIO co-leads should sustain the current JRVIO Technology Sub-committee to establish baseline standards for performance evaluation and monitoring. The same exacting criteria must measure all elements of the JRVIO. Initially, the Technology Sub-committee should focus on the following challenges:

- Software capabilities provide a host of data elements and information that when compiled may depict a measurable representation of performance for assessment.
- They must define what level of oversight or assessment is adequate to balance technical capabilities with policy standards.
- Automated monitoring software will easily provide increasing amounts of data that will require automated capabilities to analyze and assess.

C. **Public Key Infrastructure (PKI):** The Technology Sub-committee identified the requirement to protect the JRVIO from intrusion, interception, or denial of service attempts by non-authorized individuals or entities.

1. **Background:** In response to a 1997 Presidential directive DOD has established guidance for PKI as a subset of Multi-level Security (MLS) in the Defense-in-Depth[28] layered security strategy. PKI enables users of an unsecured public network to securely/privately exchange data through the use of a public/private cryptographic key pair obtained through a trusted authority. PKI allows IA services and applications to protect DOD information system transactions from unauthorized data disclosure and modification while providing positive access control to system resources. This is accomplished by user identification, user authentication, protection of data integrity, data confidentiality, and user non-repudiation. Although being revised, the DOD timeline

[27] Copyright 1998-2000, A. Jmerik. All Rights reserved.
[28] JCS//J6// Briefing PKI-Update (U)

calls for mission critical systems to utilize PKI certs/tokens by January 2003.

2. **Discussion:** The requirement for MLS is evident in the requirement for JRVIO elements to execute missions outside of existing facilities and infrastructure. PKI is not the solution for policy limitations concerning the interoperability of classified and unclassified networks. The use of PKI encryption will dramatically enhance all-source production and timeliness by providing reasonable security regardless of geographic or facility location. The following information is pertinent:

- PKI supports a level of security for low/medium risk, open-source information that when compiled and analyzed would reveal means, methods, and accuracy of JRVIO to support intelligence operations.
- PKI does not resolve the limitation placed on technology by policy.
- PKI establishes trust in cyberspace.
- PKI provides a secure end-to-end environment.
- PKI allows one level of protection within the Defense-in-Depth concept for securing cyber operations.

3. **Recommendations:** The Technology Sub-committee should:

- Monitor the use of PKI software for near-term operations as directed and ensure use by JRVIO organizations.
- Broaden its scope beyond PKI to address the complete Multi-level Security approach of the DOD Defense-in-Depth plan.

D. **Virtual Private Networks (VPN):** VPNs operate over a public network (i.e. the Internet). The purpose of the VPN is to deliver cost-effective connectivity over a wide area network (WAN). VPNs restrict unauthorized access and attempt to ensure data integrity.

1. **Background:** Virtual Private Networks (VPN) are enterprise inter-networks operated over the Internet. VPN works by using encryption to "tunnel" through switched virtual circuits (SVC) that navigate over a number of intermediary LANs in order to reach remote enterprise locations.[29] A typical VPN scenario is for an enterprise to operate through a Tier 1 Internet Service Provider (ISP) and purchase SVCs to each remote site. The SVC assures that messages will be routed in such a way that performance and security are optimized. Routers must be configured to perform the encryption and decryption operations.

2. **Observation:** VPN potentially provides a cost effective alternative to the communications infrastructure required for virtual operations while satisfying, in part, the requirements for IA safeguards. Characteristics are:

[29] Osborne / McGraw-Hill, Professional Network Library, Copyright 2000

- A VPN topology runs mostly over shared network infrastructure, usually the Internet, and has at least one private LAN segment at each end.

- VPN sessions run through an encrypted connection at each end.

- VPN provides tunneling, encryption, encapsulation, packet authentication, user authentication, and access control.

- VPN supports high-speed connectivity (DSL, Cable Modem).

- VPN requires all users to be under common security and system/network management.

- VPN initially has very complex security issues.

- The processing of high level encryption will potentially overload the client computers.

- There are substantial up-front efforts and costs for configuration and software. However, once established connection costs are lower than traditional communications support.

- It is expected that VPNs will replace WANs by the year 2003.

- With the appropriate Internet-compatible servers, firewalls, and inter-network management, VPN provides a cost-effective communications solution for JRVIO.

- A POP provided by a single or multiple commercial service providers is considered essential to the success of a VPN and its use in JRVIO operations.

3. **Recommendation:** Recommend that the Chairperson of the JRVIO Technology Sub-committee coordinate closely with DISA and the JS, J6 to evaluate this critical enabling technology for CWE. Infrastructure and architecture requirements must be identified quickly to be included with resourcing issues for the adjustments to FY 02 POM reprioritizations and/or FY03-08 POM submissions.

X. RECOMMENDATIONS:

A. **JRVIO Activation:** DEPSECDEF approve and direct activation of JRVIO organizations as described in this LRP.

B. **JRVIO Steering Group (JSG):** DEPSECDEF approve the establishment of a JSG to oversee implementation of the JRVIO LRP.

1. **Development:** The ASD/RA, ASD/C3I and Joint Staff Directors of J1, J3 and J6 will report back to DEPSECDEF within 45 days of final report approval with a recommendation on the JSG's organization and charter.

2. **Representation:** At a minimum JSG representation will include OASD/C3I, OASD/RA, JS, USSPACECOM, NSA, DISA, IOTC, the Services, the RCs and any other DOD element deemed necessary by the JSG leadership.

3. **Follow-on Issues:** The JSG has oversight of JRVIO follow-on issues as described in this report and has the authority to delegate responsibilities and tasks as required. In this case, oversight is defined as monitoring the progress of the follow-on actions cited in this report and providing advice to the authorities responsible for implementation and policy development. As a minimum, the JSG will maintain oversight of the following JRVIO issues:

- Refinement of the JRVIO CONOPS activities
- Enabling JRVIO technologies and equipment
- JRVIO support to the Unified Commands
- Joint command submission of JRVIO manpower requirements
- Training strategy for JRVIO personnel using model at Annex A-2
- Personnel management issues approved in the ILRP and listed in paragraph VIII above

4. **Sub-committees:** The JSG is authorized to establish sub-committees to monitor follow-on issues and make appropriate recommendations.

5. **Reporting:** The JSG will update the DEPSECDEF annually through FY 04 on JRVIO implementation.

C. **JRVIO CONOPS:** DEPSECDEF accept the JRVIO CONOPS as written. Acceptance of this recommendation recognizes the following:

1. The major initial JRVIO participants will be USSPACECOM (JIOC and JTF-CND), NSA, IOTC and DISA.
2. Implementation of JRVIO will be initiated by each of the participating Joint commands in accordance with plans at Annex A-1.
3. Each of the Joint command participants will submit JTMD establishment and/or expansion documents in the near term.
4. Approval also supports increased use of RC in IO activities and staffs in Unified Commands, while delaying the establishment of JRVIOs at Unified Commands pending further review and comparison of virtual IO support to Unified Commanders and their staffs from either the JIOC or from organic Unified Command RC elements.

D. **Personnel Management:** DEPSECDEF endorse the personnel management recommendations previously approved as a part of the ILRP and listed in paragraph VIII above.

E. **Resourcing:**

1. DEPSECDEF consider additional active duty manday funding in the Service active military personnel appropriations for JRVIO implementation in FY 01 and FY 02 during the FY 02 Budget Review:

	FY 01	FY 02
Mandays	$2.064M	$2.140M
O&M	-0-	$0.393M
Total	$2.064M	$2.533M

This additional funding is required to meet near-term commitments and to initiate virtual IO/IA support operations prior to the allocation of dedicated JRVIO manpower authorizations.

2. DEPSECDEF approve additional FTS personnel for these units as the concept and requirements of the mission mature in the FY 03 Program Review or Budget Review process:

FY 03	FY04	FY05	FY06	FY07
$0.663M	$0.913M	$1.178M	$1.459M	$1.692M

Drilling RC personnel required to establish JRVIO units are expected to be programmed by the Services from existing end strength resources in FY 03 and the out years. These adjustments should be made in the FY03-07 POM process.

3. Note that the manpower estimate is based on current JRVIO requirements and will be updated as the requirements are refined. The estimate represents the JRVIO force mix planned for JTMD submissions from JIOC, NSA, IOTC and DISA (including JTF-CND). The JTMD review process will allow the Services to review the manpower requirements of the five JRVIO organizations and recommend if and how these requirements could be met. The JTMD process will define the force mix and the subsequent costs associated with that construct. Some Services may plan to re-mission existing manpower to meet JRVIO requirements. Re-missioning may reduce the resource requirement. Active duty manday costs must be funded for unit OPTEMPO that cannot be accommodated within the units' annual training and normal 48 drills.

CONCEPT OF OPERATIONS
For
A Joint Reserve Virtual Information Operations (JRVIO) Organization to Support the USSPACECOM Joint Information Operations Center (JIOC)

I. **Purpose:** To create a Reserve component (RC) organization for the conduct of virtual Information Operations (IO) and related IO enabling activities in support of the USSPACECOM Joint Information Operations Center (JIOC).

II. **Mission:** The JRVIO will conduct virtual IO and enabling activities in support of JIOC's mission to provide full-spectrum IO support to Unified Commands.

III. **Functions:** The JRVIO will provide support in the following specific functional areas consistent with the assigned missions and structure of the JIOC:

A. **J3 Operations:**

1. **Exercise Augmentation:** In conjunction with the J5, provides exercise controllers, scenario scriptors, Master Scenario Events List (MSEL) developers, exercise concept development, OPFOR, Red Teaming, and White Cell support for joint exercises.

2. **Full-Spectrum IO CINC Support Team Augmentation:** Provide planning, integration and execution support to the CINCs staff across the continuum of operations.

3. **Order of Battle Maintenance:** Creation, monitoring and maintenance of intelligence databases that provide information at the level of detail and specificity to enable Information Operations planning.

4. **Specific Country Analysis:** Maintaining friendly and opposing force status and mining intelligence and intelligence related products for the purpose of assisting in the development and evaluation of IO courses of action.

5. **JRVIO Operations Coordination and Synchronization:** Full-time RC support to validate JRVIO operational requirements and evaluate JRVIO workflow and performance. Provides JRVIO mobility support. Provides direct assistance to the J3, J5 and J6 in maximally utilizing the capabilities resident in the JIOC's JRVIO.

B. **J5 Plans and Operations Support:**

1. **Defensive Information Operations (DIO):** Provide support to Unified Commands deliberate and crisis action planning; directly participate in drafting the DIO annex to Unified Command OPLANS, CONPLANS and CONOPS; participate in vulnerability assessments of Unified Commands.

2. **Rapid Access to Information Operations Information (RACI)/Open Source Information System (OSIS) Database Propagation and Maintenance:** Gather intelligence and related information to enable IO; conduct independent, all-source research and analysis of both open-source and classified information; maintain a common, joint IO information database.

3. **ACTD Threat Assessment Support:** Identify and acquire tools to satisfy analytical and collaboration requirements.

4. **Links and Nodes Data Compilation and Assessment:** Participate in the development of concepts, procedures, simulations and decision support tools for application of new IO capabilities. Maintain direct and detailed knowledge of emerging technologies that could assist in the development of IO tools and capabilities.

5. **Develop All-Source Intelligence Computer-based Training:** Use a combination of Services, agencies and JIOC developed training programs and packages to train CINC IO staffs and Unified Command senior staff members in the effective use of IO in support of a Unified Commands family of plans.

6. **Red Team Planners:** Provide exercise support by assisting in the development of the OPFOR campaign plan, MSEL and exercise injects. Serve as the focal point for facilitating and coordinating red team support from other government agencies. Participate as red cell exercise controllers.

7. **Lessons Learned Support (JIOC):** Conduct research to populate the JIOC lessons learned database. Participate in the lessons learned interview process. Coordinate with other government lessons learned agencies. Identify lessons learned for inclusion in IO doctrine and training development.

C. J6 C4 Systems:

1. **ACTD Network Modeling and Simulations:** Conduct in-depth evaluation of ACTD related information assurance planning and vulnerability assessment operations for use by CINCs, Services and Agencies.

2. **CND/CNA Technology and Technical Support:** Develop software toolkits to support the conduct of vulnerability assessments (both blue and red).

3. **Models and Tools Training Development and Conduct:** Provide direct support to CINC staffs through the use of mission-specific modeling and simulation tools and the development and maintenance of related databases.

4. **Website Maintenance:** Create and maintain SCI, collateral and unclassified websites that provide access to JIOC information and documents, and web-based modeling and simulation tools.

5. **JRVIO System Administration:** Maintain the health and welfare of the information processing, transport and storage systems that enable JRVIO operations. Provide direct support to JRVIO participants operating on the systems.

D. **J8 Programs and Resources:**

1. **JRVIO Reserve Forces Coordinator:** Function as the senior administrative and operations coordinator for the JIOC JRVIO. Design effective programs for maximal utilization of JRVIO capabilities. Develop agreements to allow JRVIO members to use existing RC infrastructure (e.g. information processing, storage and transport systems, classified and unclassified work space, etc) to conduct JRVIO operations with minimal resourcing impact on the JIOC.

2. **JRVIO Resources Coordinator:** Provides personnel, fiscal and logistics management support particular to JRVIO.

E. **J9 Technology and Operational Demonstration:** TBD

IV. **Organization & Management:**

A. **Location:** The JRVIO will consist of RC personnel performing assigned missions and tasks both onsite at the JIOC, Kelley AFB, San Antonio, Texas, and from remote sites across CONUS employing virtual operations techniques and technologies.

B. **C2:** Members of the RC assigned to the JIOC JRVIO will be under the operational control of the JIOC, and assigned to the JIOC for their primary peacetime, contingency, crisis or wartime missions (i.e. war-traced to the JIOC). The JIOC JRVIO, as per normal Joint RC procedures, will rely on the JIOC JRVIO Reserve Forces Coordinator and parent RC Commanders to provide administrative control in accordance with Service procedures and pre-existing arrangements.

C. **Operational Concept:** Operational control will flow from the supported JIOC staff element to the JRVIO through the JRVIO coordination element in the JIOC J3. The three full time JRVIO personnel in the J3 provide operations coordination and synchronization. They are not meant to impede access to JRVIO capabilities but operate to ensure maximal utilization of JRVIO capabilities. They will seek to match JRVIO capabilities to existing requirements. In those instances where routine procedures and relationships have developed between JRVIO members/elements with individual JIOC staff sections, the J3 coordination and synchronization team will not operate to impede or hamper those relationships. In terms of administrative control, the JIOC JRVIO Reserve Coordinator's Office will provide administrative support, managerial direction and operational focus to the overall JIOC JRVIO organization via a small, RC-staff subordinate to the JIOC J8. The JIOC JRVIO Reserve Forces Coordinator will work tirelessly to identify and access appropriate JRVIO personnel and to enable JRVIO operations at minimal cost to the JIOC via utilization of existing RC systems, equipment and facilities infrastructure. The parent RC will provide administrative control over Service-specific matters. Depending upon the specific mission requirement and the RC affiliation, JIOC JRVIO

members may be required to deploy to perform assigned functions either on-site at the JIOC, or potentially deployed to an AOR in support of a Combatant Command should extraordinary circumstances dictate. Some training for JRVIO members will be required on-site. However, under routine operational conditions the normal mode of operation for the JIOC JRVIO will be to accomplish its required training, administration and assigned missions, tasks and activities virtually from distant collective or individual duty sites from the supported JIOC staff element. Under this operational concept mission tasking, oversight, quality control, and fulfillment is envisioned to be accomplished via communications links established between the JRVIO and the supported JIOC staff element or Combatant Command to make maximum use of information technologies such as computer video-teleconferencing, collaborative electronic workspaces, multi-level security and encryption, and electronically-shared files and directories. It must be clear that the JIOC JRVIO is under the operational control of the JIOC for all states of the environment and is fully and completely war-traced to the JIOC. No other end-state arrangement is acceptable. The sensitive and complex nature of Unified Command IO demands such an arrangement. The JIOC will certify JRVIO individuals to operate virtually. While the conduct of virtual operations is the desired and envisioned end-state, pre-certification training on site at the JIOC will be required. It is entirely possible and indeed probable, that individuals and elements of the JIOC JRVIO located in the greater San Antonio area will operate out of the recently established Joint IO Center in Building 178 on Lackland Air Force Base. These personnel, while located physically close to the JIOC HQ on Kelley Air Force Base, will none the less be operating virtually and should be included in the JRVIO.

D. **Functional Nature and Staffing Arrangements:**

1. **JIOC Staff Directorates:** JRVIO members will be accessed and allocated to specific directorates within JIOC (i.e., J3/5/6/8) based on mission support agreements. These agreements will identify the mission support requirements and define in detail how the JRVIO plans to meet those requirements. Based on these agreements, JRVIO Operations Managers from the J3 (three full time RC personnel) will coordinate non-routine mission support activities of the JRVIO with the appropriate staff directorate commander or designated representative. While assigned to JIOC, the JRVIO is envisioned to be an integral part of the larger JIOC Joint Reserve Program (to be established).

2. **JRVIO Management Cell:** A JRVIO Management Cell will be located at JIOC Headquarters within the J8. Full-time support positions are required to coordinate JRVIO activities and to interface with JIOC active duty and civilian senior leadership. Two positions, the JRVIO Reserve Coordinator and a JRVIO Resources Coordinator are envisioned. These positions will be the key link between the JIOC senior leaders and JRVIO Operations Managers. The JRVIO Resources Coordinator will coordinate with respective RC headquarters on all personnel and manpower matters such as, personnel staffing, performance, training, career progression, assignment rotation, etc. The requirement for JRVIO full-time support will be a total of 5 RC personnel (two in the J8 and three in the J3).

V. **Responsibilities:**

A. **Military Services:**

1. Provide RC personnel resources to JIOC for staffing of the JRVIO.
2. Realign manpower and funding from identified sources to the JRVIO with routine administrative control maintained by the parent RC Service.
3. Recruit and hire highly skilled personnel according to JIOC mission requirements.
4. Fund all reserve military personnel pay and allowances.
5. After initial mission orientation and training, ensure JRVIO personnel maintain readiness posture as defined by Designed Operational Capability Statements.
6. Provide facilities for the JRVIO participants to perform their administrative functions

B. **Director, JIOC:**

1. Serve as the Executive Agent for the JRVIO.
2. Provide the facilities and other administrative requirements to support the JRVIO, and/or establish any required Memorandum of Understanding for facility or administrative support with the DoD locations from which the JRVIO will operate.
3. Develop an implementation plan and Standard Operating Procedures (SOP).
4. Identify, as appropriate, current and/or additional requirements.
5. Evaluate funding adequacy and support requirements for the JRVIO.
6. Assist Services during their recruitment processes by providing mission requirements such as, position and skill set descriptions.
7. Activate the JRVIO Management Cell from resources provided by the Services.
8. Fund any necessary JRVIO participant travel, per diem, equipment, and training expenses not routinely funded by the Services.
9. Provide for utilization of the necessary facilities and equipment to train for and perform the JIOC mission. The type of equipment (hardware and/or software) is dependent on the mission area supported.
10. Provide necessary initial and recurring training for the element personnel.
11. Provide for the technical proficiency and tactical competence of all assigned members.
12. Provide for the management of JRVIO training and exercises planning and coordination. Management includes the scheduling and coordination of training and exercises with CINCs, and other organizations.

VI. **JIOC JRVIO Stand-Up Timeline:** The functions annotated with "(IOC)" are required for the JRVIO to meet its responsibilities for IOC.

A. Establish specific functional tasks. (IOC)

B. Develop the staffing plan by skill for each billet. (IOC)

C. Develop budgetary program lines for inclusion in the ASD/RA POM. (IOC)

D. Submit manpower requirements for Service approval. (IOC)

E. Develop appropriate MOA/MOUs as necessary between JIOC and other organizations. (IOC)

F. Secure required equipment for JRVIO as required. (IOC)

G. In conjunction with the RC and military departments identify personnel to meet requirements. (IOC)

H. Develop long-range acquisition strategy to support and improve virtual operations. (FOC)

ADDENDUMS

A. Staffing:

JIOC JRVIO MANPOWER REQUIREMENTS STAFFING:

[1]

Full Time Support:		**FY03**	**FY04**	**FY05**	**FY06**	**FY07**	**FY08**
AFRC							
Officer		2	2	2	2	2	2
USAR							
Officer		1	1	1	1	1	1
USNR							
Officer		1	1	1	1	1	1
USMCR							
Enlisted		1	1	1	1	1	1
Total		**5**	**5**	**5**	**5**	**5**	**5**
Drilling Reservists:							
USAR							
Officer		26	26	26	26	26	26
Enlisted		14	14	14	14	14	14
AFRC							
Officer		35	35	35	35	35	35
Enlisted		13	13	13	13	13	13
USNR							
Officer		35	35	35	35	35	35
Enlisted		10	10	10	10	10	10
USMCR							
Officer		9	9	9	9	9	9
Enlisted		2	2	2	2	2	2
Total		**144**	**144**	**144**	**144**	**144**	**144**

[1] While the JIOC would like JRVIO personnel in ’01, the first POM submission that they can effect is ’03 and therefore the resourcing timeline runs over the FYDP from ’03 – ’08.

B. Resources: The JRVIO will train and operate with hardware and software that are contained within established facilities capable of hosting JIOC JRVIO personnel. This utilization of existing facilities will mitigate standing up new sites across the country. However, if additional equipment is required for JIOC JRVIO-specific missions, the JIOC and facility senior leadership will work together to acquire the necessary equipment to perform the missions.

C. **Security:** It is envisioned that JRVIO personnel supporting the JIOC will require a Top Secret/Special Compartmented Information (TS/SCI) clearance. While it is acknowledged that some of the missions may be conducted in a collateral or even unclassified environment, a TS/SCI clearance is necessary to provide the appropriate level of mission briefing prior to executing the mission.

CONCEPT OF OPERATIONS

For

A Joint Reserve Virtual Information Operations (JRVIO) Organization to Support the Joint COMSEC Monitoring Activity (JCMA) of the Defensive Information Operations Group at the National Security Agency (NSA)

I. **Purpose:** To enhance an existing JCS/NSA Reserve Component (RC) organization for virtual performance of Information Assurance (IA) operations in support of the unified commands, government agencies, and other customers.

II. **Mission:** The JRVIO will be integrated with the JCMA for planning, directing, and executing COMSEC Monitoring of DoD telecommunications, automated information systems, and communications signals.

III. **Functions:** The JRVIO will provide support in the following specific functional areas consistent with the assigned missions and structure of the JCMA:

A. **JCMA Current Operations Division:** Conduct long and short term mission planning as well as long term analysis of the impact of discovered vulnerabilities as they relate to operations. Analyze technology and policy implications for information systems security. Train personnel for COMSEC and Force Protection operations. Coordinate development of agreements for the conduct of JCMA operations. Conduct RCMC tasking as well as reporting on discovered vulnerabilities and provide 24x7 operations in crises/contingencies.

B. **Regional COMSEC Monitoring Center (RCMC):** Provide reporting and analysis to JCMA current operations and to the CMOC as well as to sister RCMCs on occasion.

C. **Joint COMSEC Monitoring and Analysis Team (JCMAT):** Provide support to CINCs during exercises and /or contingency operations.

IV. **Organization & Management:**

A. **Authorities:**

1. Electronic Communications Privacy Act

2. EO 12333, United States Intelligence Activities

3. NSD 42, National INFOSEC Policy

4. NTISSD 600, COMSEC Monitoring

5. DOD DIRs 5200.5 and 4640.6, COMSEC Monitoring in DoD

B. **Location:** The JRVIO will consist of RC personnel performing assigned missions and tasks both on site at JCMA current operations division, FANX3, Linthicum, Maryland and from remote sites across CONUS and OCONUS employing virtual operations techniques and technologies. JCMA locations are distributed as follows:

1. JCMA Current Ops, ISSO, FANX3, Linthicum, Maryland

2. RCMC, Kent Island, Maryland

3. RCMC, Camp Parks, California

4. RCMC, Camp H.I. Smith, Hawaii

5. RCMC, Bad Aibling, Germany

6. RCMC, Menwith Hill, England

7. JCMATs, Worldwide

C. **C2:** Members of the RC assigned to the JCMA JRVIO will be under the operational control of the JCMA and assigned to the JCMA for their primary peacetime, contingency, crisis or wartime missions (i.e. war-traced to the JCMA). The JCMA JRVIO will rely on the JRVIO management cell and parent RC Commanders to provide administrative support of drilling reservists in accordance with Service procedures and pre-existing arrangements.

D. **Operational Concept:** The supported JCMA staff element will exercise total operational control over the JRVIO. In terms of administrative control, the JRVIO management cell in JCMA will provide administrative support to the overall JCMA organization. The JRVIO management cell will work to identify and access appropriate JRVIO personnel using existing RC systems, equipment and facilities infrastructure. The parent RC will provide administrative control over Service-specific matters. The JRVIO management cell will seek to match JRVIO capabilities to existing requirements. In those instances where routine procedures and relationships have developed between JCA and JRVIO members/elements, the JRVIO management cell will not operate to impede or hamper those relationships. Depending on the mission requirements and the RC affiliation, JCMA JRVIO members may be required to deploy to perform assigned duties either to one of the locations described above or to an AOR in support of Combatant Commands should extraordinary circumstances dictate. Training of JRVIO members will be required on site. Under this operational concept, mission tasking, oversight, quality control and accomplishment is envisioned via communications links established between the JRVIO and the supported JCMA staff element to make maximum use of information technologies such as computer video teleconferencing, collaborative electronic workspaces, encryption and electronically shared files and directories. The JCMA JRVIO command and control (C2) relationships internal and external are consistent with those of other, non-virtual RC units. Command and control will be exercised as in any existing reserve chain of command. The supported organization will assign missions to the supporting organization for their primary peacetime missions. Upon mobilization, operational control (OPCON) will be exercised by the commander designated to receive OPCON by the Secretary of Defense or,

when authorized, by the appropriate combatant commander. The JCMA JRVIO is war-traced to the JCMA.

E. **Functional Nature and Staffing Arrangements:**

1. **JCMA Elements:** JRVIO members will be accessed and allocated to specific groups within the JCMA (i.e., Current Ops Division/RCMC/JCMAT) based on mission support agreements. These agreements will identify the mission support requirements and define in detail how the JRVIO plans to meet those requirements. Although assigned to JCMA, the JRVIO is envisioned to be an integral part of the larger NSA Joint Reserve Program.

2. **JRVIO Management Cell:** A JRVIO management cell will be located at JCMA Headquarters. Full-time support positions are required to coordinate JRVIO activities and to interface with JCMA active duty and civilian senior leadership. Additionally, a JRVIO Program Coordinator will provide the key mission link between the JCMA senior leaders and JRVIO personnel. A JRVIO Resources Coordinator will coordinate with respective RC Headquarters on all personnel and manpower matters such as, personnel staffing, performance, training, career progression, assignment rotation, etc.

V. **Responsibilities:**

A. **Military Services:**

1. Provide RC personnel resources to NSA for staffing of the JRVIO.
2. Provide staffing and fund FTS positions in the JRVIO Management Cell.
3. Realign manpower and funding from identified sources to the JRVIO with routine administrative control maintained by the parent RC Service.
4. Recruit and hire highly skilled personnel according to JCMA mission requirements.
5. Fund all Reserve military personnel pay and allowances.
6. After initial mission orientation and training, ensure JRVIO personnel maintain readiness posture as defined by Designed Operational Capability Statements.
7. Provide facilities for the JRVIO participants to perform their administrative functions

B. **Director, JCMA:**

1. Serve as the Executive Agent for the JCMA JRVIO mission.
2. Provide the facilities and other administrative requirements to support the requisite JRVIO mission elements, and/or establish any required Memorandum of Understanding for facility or administrative support with the DoD locations from which the JRVIO teams will operate.
3. Develop an implementation plan and Standard Operating Procedures (SOP).

4. Identify, as appropriate, current and/or additional requirements.
5. Evaluate funding adequacy and support requirements for the JRVIO.
6. Assist Military Services during their recruitment processes by providing mission requirements such as position and skill set descriptions.
7. Activate the JRVIO Management Cell from resources provided by the Services.
8. Fund any necessary JRVIO participant operational travel, per diem, equipment, and training expenses not routinely funded by the Services.
9. Provide for utilization of the necessary facilities and equipment for training and performance of assigned missions. The type of equipment (hardware and/or software) is dependent on the mission area supported.
10. Provide necessary initial and recurring training for the element personnel.
11. Provide for the technical proficiency and tactical competence of all assigned members.
12. Provide for the management of JRVIO training and exercises planning and coordination. Management includes the scheduling and coordination of training and exercises with CINCs and other organizations.

VI. Organizational Stand-Up Timeline:

A. **Initial Operational Capability:** The functions listed below will constitute the JRVIO initial operational capability.

1. Provide direct support to customers through the RCMC at Camp Parks, CA.
2. Conduct long and short term mission planning.
3. Provide support to the CMOC in tasking RCMC activities and assessing their reporting.
4. Participate in joint training exercises.
5. Provide ongoing technical training to increase proficiency of assigned JRVIO personnel.

B. **Full Operational Capability:** The functions listed below will constitute the JRVIO full operational capability.

1. Develop contingency plans, tactics, techniques, and procedures to defend DOD information systems and networks.
2. Provide training to Active Duty personnel for COMSEC and Force Protection operations.
3. Provide virtual staff augmentation to the additional RCMC sites.

ADDENDUMS

A. Staffing:

NSA JCMA JRVIO MANPOWER REQUIREMENTS STAFFING[1]:

Full Time Support:		**FY03**	**FY04**	**FY05**	**FY06**	**FY07**	**FY08**
AFRC							
Officer		1	1	1	1	1	1
ARNG							
Officer		1	1	1	1	1	1
USMCR							
Officer							
USNR							
Officer							
Enlisted		1	1	1	1	1	1
Total		**3**	**3**	**3**	**3**	**3**	**3**
Drilling Reservists:							
USAR							
Officer		2	2	2	2	2	2
Enlisted		7	7	7	7	7	7
ARNG							
Officer		6	6	6	6	6	6
Enlisted		11	11	11	11	11	11
AFRC							
Officer		8	8	8	8	8	8
Enlisted		36	36	36	36	36	36
USNR							
Officer		16	16	16	16	16	16
Enlisted		72	72	72	72	72	72
USMCR							
Officer		6	6	6	6	6	6
Enlisted		11	11	11	11	11	11
Total		**175**	**175**	**175**	**175**	**175**	**175**

[1] While the JCMA would like JRVIO personnel in ’01, the first POM submission that they can effect is ’03 and therefore the resourcing timeline runs over the FYDP from ’03 – ’08.

B. **Resources**: The JRVIO will train and operate with hardware and software that are contained within established facilities capable of hosting JCMA JRVIO personnel. However, if additional equipment is required for JCMA JRVIO-specific missions, the JCMA and facility senior leadership will work together to acquire the necessary equipment to perform the missions.

C. **Security:** It is envisioned that JRVIO personnel supporting the JCMA will require a Top Secret/Sensitive Compartmented Information (TS/SCI) clearance. While it is acknowledged that some of the missions may be conducted in a collateral or even unclassified environment, a TS/SCI clearance is necessary to provide the appropriate level of mission briefing/training prior to executing the mission.

CONCEPT OF OPERATIONS
for
A Joint Reserve Virtual Information Operations (JRVIO) Organization to Support the Information Operations Technology Center (IOTC)

I. **Purpose:** To create a Reserve component (RC) organization for the conduct of virtual Information Operations (IO) and related IO enabling activities in support of the Information Operations Technology Center (IOTC).

II. **Mission:** The JRVIO will conduct virtual IO and enabling activities in support of IOTC's mission to provide IO support to DOD and the Intelligence Community.

III. **Functions:** The JRVIO will provide support in the following specific functional areas consistent with the assigned missions and structure of the IOTC:

A. **Community Coordination Group (CCG):**

1. **Technology Sharing:** Promote and facilitate technology sharing and information exchange in concert with the Advance Technology Group. Participate in new and existing community, technology sharing.

2. **Requirements Coordination:** Coordinate external tasking through appropriate mechanisms. Provide staff support to the DOD/IC Steering Group decision-making process. Oversee technology and technical data exchanges between developers and customers.

3. **Planning, Exercise, and Operations Support:** Provide direct planning, exercise and operations IO technology support to DOD and Intelligence Community.

B. **Analysis and Assessment Group (AAG):**

1. **Systems and Vulnerability Analysis:** Combine information system infrastructure and technical vulnerability assessment in support of IO.

2. **Modeling and Simulation:** Apply modeling and simulation tools to verify results of analysis, and facilitate isolation of technical vulnerabilities.

3. **Technical Analytic Support:** Provide technical assistance in support of operational planning.

IV. Advance Technology Group (ATG):

1. **Technology Analysis:** In coordination with the Analysis and Assessment Group and the DOD/IC analytic elements conduct technology analysis assessment and forecasts to identify current and emerging technologies relevant to IO.

2. **Technique Development:** Develop and apply telecommunications and computer technologies to national security problems in the IO arena.

3. **Technical Support:** Provide technical assistance in support of DOD and IC activities.

V. **Organization & Management:**

A. **Location:** The JRVIO will consist of RC personnel performing assigned missions and tasks both onsite at the IOTC, Ft. Meade, Maryland, and from remote sites across CONUS employing virtual operations techniques and technologies.

B. **C2:** Members of the RC assigned to the IOTC JRVIO will be under the operational control of the IOTC, and assigned to the IOTC for their primary peacetime, contingency, crisis or wartime missions (i.e. war-traced to the IOTC). The IOTC JRVIO, as per normal Joint RC procedures, will rely on the IOTC JRVIO Reserve Management Office and parent RC commanders to provide administrative control in accordance with Service procedures and pre-existing arrangements.

C. **Operational Concept:** Operational control will flow from the supported IOTC Groups to the JRVIO through the JRVIO Operations Coordinator in the IOTC Reserve Management Office (to be established). The JRVIO Operations Coordinator provides operations coordination and synchronization. The position is not meant to impede access to JRVIO capabilities but operate to ensure maximal utilization of JRVIO capabilities. The JRVIO Operations Coordinator will seek to match JRVIO capabilities to existing requirements. In those instances where routine procedures and relationships have developed between JRVIO members/elements with individual IOTC Groups, the JRVIO Operations Coordinator will not operate to impede or hamper those relationships. In terms of administrative control, the IOTC JRVIO Reserve Management Office will provide administrative support, managerial direction and operational focus to the overall IOTC JRVIO organization via a JRVIO Resources Coordinator. The IOTC JRVIO Reserve Management Office will work to identify and access appropriate JRVIO personnel and to enable JRVIO operations at minimal cost to the IOTC via utilization of existing RC systems, equipment and facilities infrastructure. The parent RC will provide administrative control over Service-specific matters. Some training for JRVIO members may be required on-site. However, under routine operational conditions the normal mode of operation for the IOTC JRVIO will be to accomplish its required training, administration and assigned missions, tasks and activities virtually from collective or individual duty sites distant from the supported IOTC Group. Under this operational concept, mission tasking, oversight, quality control, and requirements execution is envisioned to be accomplished via communications links established between the JRVIO and the supported IOTC Group making maximum use of information technologies such as computer video-teleconferencing, collaborative electronic workspaces, multi-level security and encryption, and electronically-shared files and directories. The IOTC JRVIO command and control (C2) relationships internal and external are consistent with those of other, non-virtual RC units. Command and control will be exercised as in any existing reserve chain of command. The supported organization will assign missions to the supporting organization for their primary peacetime missions. Upon mobilization, operational control (OPCON) will be exercised by the commander designated to receive OPCON by the Secretary of Defense or, when authorized, by the appropriate combatant

commander. The IOTC JRVIO is war-traced to the IOTC. The IOTC will certify JRVIO individuals to operate virtually. While the conduct of virtual operations is the desired and envisioned end-state, pre-certification training on site at the IOTC may be required.

D. **Functional Nature and Staffing Arrangements:**

1. **IOTC Groups:** JRVIO members will be accessed and allocated to specific groups within IOTC (i.e., CCG/AAG/ATG) based on mission support agreements. These agreements will identify the mission support requirements and define in detail how the JRVIO plans to meet those requirements. Based on these agreements, the Reserve Management Office (to be established) will coordinate non-routine mission support activities of the JRVIO with the appropriate group commander or designated representative. While assigned to IOTC, the JRVIO is envisioned to be an integral part of the larger IOTC RC Support Element (to be established).

2. **JRVIO Management Cell:** A JRVIO Management Cell will be located at IOTC Headquarters within the Reserve Management Office. Full-time support positions are required to coordinate JRVIO activities and to interface with IOTC active duty and civilian senior leadership. Two positions, the JRVIO Operations Coordinator, serving as the Deputy Commander of the IOTC RC Support Element, (to be established) and a JRVIO Resources Coordinator are envisioned. These positions will be the key link between the IOTC senior leaders and JRVIO personnel. The JRVIO Resources Coordinator will coordinate with respective RC headquarters on all personnel and manpower matters such as, personnel staffing, performance, training, career progression, assignment rotation, etc. The requirement for JRVIO full-time support will be a total of 2 RC personnel (1 Officer serving as the JRVIO Operations Coordinator and 1 Enlisted serving as the JRVIO Resources Coordinator).

VI. **Responsibilities:**

A. **Military Services:**

1. Provide RC personnel resources to IOTC for staffing of the JRVIO.
2. Realign manpower and funding from identified sources to the JRVIO with routine administrative control maintained by the parent RC Service.
3. Recruit and hire highly skilled personnel according to IOTC mission requirements.
4. Fund all reserve military personnel pay and allowances.
5. After initial mission orientation and training, ensure JRVIO personnel maintain readiness posture as defined by Designed Operational Capability Statements.
6. Provide facilities for the JRVIO participants to perform their administrative functions

B. **Director, IOTC:**

1. Serve as the Executive Agent for the JRVIO.
2. Provide the facilities and other administrative requirements to support the JRVIO, and/or establish any required Memorandum of Understanding for facility or administrative support with the DOD locations from which the JRVIO will operate.
3. Develop an implementation plan and Standard Operating Procedures (SOP).
4. Identify, as appropriate, current and/or additional requirements.
5. Evaluate funding adequacy and support requirements for the JRVIO.
6. Fund FTS positions.
7. Assist Services during their recruitment processes by providing mission requirements such as, position and skill set descriptions.
8. Activate the JRVIO Management Cell from resources provided by the Services.
9. Fund any necessary JRVIO participant travel, per diem, equipment, and training expenses not routinely funded by the Services.
10. Provide for utilization of the necessary facilities and equipment to train for and perform the IOTC mission. The type of equipment (hardware and/or software) is dependent on the mission area supported.
11. Provide necessary initial and recurring training for the element personnel.
12. Provide for the technical proficiency and tactical competence of all assigned members.
13. Provide for the management of JRVIO training and exercises planning and coordination. Management includes the scheduling and coordination of training and exercises with CINCs, and other organizations.

VII. **IOTC JRVIO Stand-Up Timeline:** The functions annotated with "(IOC)" are required for the JRVIO to meet its responsibilities for IOC.

A. Establish specific functional tasks. (IOC)

B. Develop the staffing plan by skill for each billet. (IOC)

C. Develop budgetary program lines for inclusion in the ASD/RA POM. (IOC)

D. Submit manpower requirements for Service approval. (IOC)

E. Develop appropriate MOA/MOUs as necessary between IOTC and other organizations. (IOC)

F. Secure required equipment for JRVIO as required. (IOC)

G. In conjunction with the RC and military departments identify personnel to meet requirements. (IOC)

H. Develop long-range acquisition strategy to support and improve virtual operations. (FOC)

ADDENDUMS

A. Staffing:

IOTC JRVIO MANPOWER REQUIREMENTS STAFFING[1]:

Full Time Support:		**FY03**	**FY04**	**FY05**	**FY06**	**FY07**	**FY08**
AFRC							
Officer		1	1	1	1	1	1
USNR							
Enlisted		1	1	1	1	1	1
Total		**2**	**2**	**2**	**2**	**2**	**2**
Drilling Reservists:							
USAR							
Officer		10	10	10	10	10	10
Enlisted		6	6	6	6	6	6
AFRC							
Officer		10	10	10	10	10	10
Enlisted		6	6	6	6	6	6
USNR							
Officer		6	6	6	6	6	6
Enlisted		6	6	6	6	6	6
USMCR							
Officer		4	4	4	4	4	4
Enlisted		2	2	2	2	2	2
Total		**50**	**50**	**50**	**50**	**50**	**50**

B. **Resources:** The JRVIO will train and operate with hardware and software that are contained within established facilities capable of hosting IOTC JRVIO personnel. Utilization of existing facilities will mitigate standing up new sites across the country. However, if additional equipment is

[1] While the IOTC would like JRVIO personnel in ’01, the first POM submission that they can effect is ’03 and therefore the resourcing timeline runs over the FYDP from ’03 – ’08.

required for IOTC JRVIO-specific missions, the IOTC and facility senior leadership will work together to acquire the necessary equipment to perform the missions.

C. **Security:** It is envisioned that JRVIO personnel supporting the IOTC will require a Top Secret/Special Compartmented Information (TS/SCI) clearance. While it is acknowledged that some of the missions may be conducted in a collateral or even unclassified environment, a TS/SCI clearance is necessary to provide the appropriate level of mission briefing prior to executing the mission.

CONCEPT OF OPERATIONS
For
A Joint Reserve Virtual Information Operations (JRVIO) Organization to Support the Defense Information Systems Agency (DISA)

I. **Purpose:** To create a Reserve component (RC) organization for virtual performance of IO and related activities in support of the Defense Information Systems Agency (DISA).

II. **Mission:** The JRVIO will assist DISA in coordinating, directing, planning and executing the defense of information, information systems and computer networks comprising the Defense Information Infrastructure (DII) from strategic and localized CNA and Computer Network Exploitation (CNE). This mission includes the coordination of DOD defensive actions with non-DOD government agencies and appropriate private organizations.

III. **Functions**: The JRVIO will perform tasks as directed by DISA in support of the JTF-CND and the DOD CERT. Detailed descriptions of tasks and functions are specified below.

A. **New Tool, Technique And Vulnerability Discovery:** The JRVIO will monitor publicly accessible computer networks, web sites, chat rooms, bulletin boards, and newsgroups to discover new tools, techniques and vulnerabilities.

B. **Tool, Technique and Vulnerability Analysis:** Tools, techniques, and vulnerabilities uncovered during the discovery phase of JRVIO operations will be analyzed to identify whether it works as claimed and what platforms or operating systems, application programs, or environments may be affected. A database of results and findings will be maintained and vulnerability bulletins will be issued as vulnerabilities are revealed.

C. **IAVA Compliance Verification:** In support of the DOD CERT, the JRVIO will verify compliance with directives outlining patches to known vulnerabilities for DOD components.

1. **Vulnerability Assessments:** As directed by DISA, the JRVIO will schedule and perform computer systems and networks vulnerability assessments on request from DOD components. The JRVIO will report its findings to the requesting organization.

D. **Direct JTF-CND Staff Augmentation**: The JRVIO will directly augment JTF-CND operations with watch officers and intelligence analysts performing their duties using virtual operations techniques. JRVIO personnel will increase the JTF-CND ability to determine when systems are under attack, assess the impact on military operations and capabilities, coordinate and direct appropriate DOD actions to respond to an attack, contain damage, and restore functionality.

E. **Direct GNOSC Staff Augmentation:** A JRVIO element will complement weekend (2x24) operations within the GNOSC Command Center through virtual support techniques. The JRVIO personnel in this capacity will assist the GNOSC mission is to manage, control, monitor, and protect essential elements and applications of the DII in

order to ensure its availability to support the needs of the National Command Authority, CINCs, Services, agencies, and "the war-fighters."

1. Direct RNOSC Staff Augmentation: JRVIO elements will be assigned to the Scott RNOSC and PAC RNOSC to complement full-time weekend (2x24) operations using virtual operations techniques similar to the support provided to the GNOSC. These JRVIO personnel will provide a single point of contact for the theater CINC, Services, and Agencies for network, systems, applications, services, and information status and anomalies. During crisis or other surge operations the JRVIO members will facilitate full-time daily (7x24) operations at these RNOSCs. The JRVIO elements supporting the CENT and EUR RNOSCs will train with the CONUS RNOSC JRVIO elements and therefore, will complement the weekend (2x24) operations at the CONUS RNOSCs. When activated, these two JRVIO elements will complement (7x24) operations at their overseas mission locations. The end objective for these elements is to train and be ready to support any RNOSC requiring mission support.

2. **JWRAC Augmentation: JRVIO** personnel will support and extend the analysis capabilities of the JWRAC.
3. **Web log Analysis: JRVIO** personnel will providing site log and traffic analysis virtually.

4. **Exercise Participation:** The JRVIO will participate in selected joint training exercises to augment an exercise Information Assurance (IA) blue team, to perform or augment IO red team duties, or to provide the IO/IA controller or white team.

IV. **Organization & Management:**

A. **Location:** JRVIO elements and personnel will support DISA operations and missions in a variety of CONUS and OCONUS locations as follows:

1. **JRVIO Unit Location:** Andrews AFB, MD in support of the JTF-CND Operations Center; at HQ DISA, Arlington, VA
2. **JRVIO Unit Location:** Andrews AFB, MD in support of the DISA Operations Directorate (D3) Global Network Operations and Security Center (GNOSC) at HQ DISA, Arlington, VA
3. **JRVIO Unit Locations:** Scott AFB, IL and Wright-Patterson AFB, OH in support of the *DISN Service Center,* Scott RNOSC at Scott AFB, IL
4. **JRVIO Unit Locations:** Scott AFB, IL in support of the DISA CENTCOM RNOSC located in Bahrain.
5. **JRVIO Unit Location:** Columbus, OH in support of the DISA EUCOM RNOSC located in Germany.
6. **JRVIO Unit Location:** Hickham AFB, HI in support of the DISA PACOM RNOSC locate at Wheeler AAF, HI.

7. **Individual JRVIO** members will function as Watch Officers and provide intelligence analysis, OPSEC, CND analysis and planning support from various remote sites to include JRICs, other government facilities and personal residences.

B. **Command and Control:** Command of all JRVIO elements in support of DISA will remain with the respective Reserve component at this time. Operational Control (OPCON) will be exercised by the supported entity. For example, the Commander JTF-CND exercises OPCON over the JRVIO element assigned to support the JTF-CND, while the DISA Reserve Coordinator will exercise Administrative Control (ADCON) for this element. The other JRVIO elements included in this CONOP will remain under the OPCON of the appropriate element of DISA they support, while relying on the DISA Reserve Coordinator and parent RC commander to provide ADCON in accordance with pre-existing arrangements The following diagram depicts these command relationships.

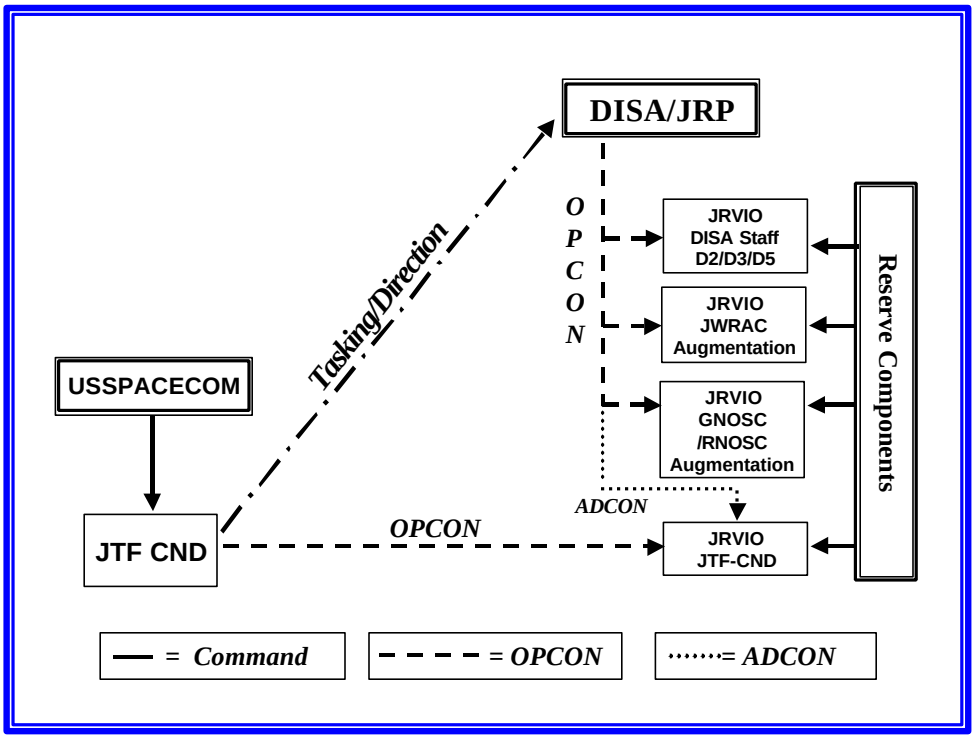

Figure 1 – Command and Control Relationships

1. **Defense Information Systems Agency (DISA):** The JRVIO command function will be co-located with and hosted by DISA, which will serve as the Support Agency. The Director, DISA is designated the Executive Agent for the JRVIO. On a daily basis, JRVIO will be in direct support of the JTF-CND and DISA organizations tasked with the defense of DOD computer systems and networks. DISA will provide: administrative, logistics, resource management, PA, general counsel and personnel support. During periods of extended CNA where the JRVIO is augmenting the JTF-CND and DISA activities, DISA will provide operational and administrative support to the fullest extent possible.

2. **Other Agencies: The** JRVIO will utilize DISA's standing relationships for law enforcement activities through the Defense Criminal Investigative Service (DCIS) and CI activities through the JTF-CND Staff CI Officer.

C. **Operational Concept:** The JRVIO is a deployable asset but deployments may actually be "virtual" as individuals may accomplish tasks at one location while actually being physically located at another. The JRVIO may be employed in a wide range of contingencies while supporting the JTF-CND in CND operations on an ongoing basis. Individuals and units may be employed by their respective reserve component for this purpose and, in fact, this is one of the primary purposes of the JRVIO – to provide each reserve component with the expertise necessary to support their own CND efforts. The JRVIO may be assigned in a direct support capacity to a Unified command for limited periods.

1. **Command Group:** The Command Group includes the Commander, Deputy Commander, J1/J4/J8, and administrative support personnel. The Commander, JRVIO will be responsible for the overall execution of the policies, procedures, and operations of the JRVIO. The Deputy Commander will be responsible for the day-to-day functions of JRVIO serving as the focal point for synchronization of the staff, exercising daily operational authority over the JRVIO on behalf of the commander. The J1/J4/J8 will provide critical liaison functions with DISA for administration, logistics, PA, and resource management and will manage the day-to-day administration requirements for JRVIO**.**

2. **Joint Reserve Program (JRP):** DISA's Joint Reserve Program is comprised of all six DOD Reserve components. Various units and or individuals from this pool of RC personnel will perform staff augmentation to the JTF-CND, GNOSC, and RNOSCs, as well as, IAVA Compliance Verification, Exercise Support, and Tool, Technique and Vulnerability Analysis. Direction will come from the JTF-CND or DISA element exercising operational control over the unit or individual.

3. **Joint Web Risk Assessment Cell (JWRAC):** The JWRAC is the primary DOD organization for cross-component OPSEC, vulnerability analyses, and threat assessments of Web content on DOD publicly accessible Web sites. In this role, the JWRAC will accomplish OPSEC, vulnerability analyses and threat assessments of the content and data resident on publicly accessible unclassified DOD Web sites from a joint, cross-component perspective using the OPSEC process.

4. **Web log Analysis: JRVIO** personnel will providing site log and traffic analysis virtually. These personnel will be separate from the JWRAC and JRP. Personnel will be drawn from all Services. Tasking will come directly from the D33 at DISA.

D. **Functional Nature and Staffing Arrangements:**

1. **DISA Operations Centers/Commands:** JRVIO elements will be attached to specific Operation Centers/Commands within DISA based on mission support agreements

signed by the appropriate JRVIO element chiefs, the Mobilization Assistant to the DISA Director, and the respective DISA Operation Center/Command Commanders. These agreements will identify the mission support requirements and define in detail how the JRVIO elements plan to meet those requirements. Based on these agreements, JRVIO element chiefs will coordinate all day-to-day mission support activities of the elements with the appropriate Operation Center/Command Commander or designated representative. While assigned to DISA, the JRVIO elements will be an integral part of the DISA JRP and therefore, element chiefs will also coordinate all mission support activities with the DISA JRP senior leadership.

2. **JRVIO Management Cell:** A JRVIO Management Cell will be located at DISA Headquarters. Full-time support positions are required to coordinate JRVIO element activities and to interface with DISA active duty and reserve senior leadership. These positions will be provided by DISA and will be the key link between the DISA senior leaders and JRVIO element chiefs. JRVIO element chiefs will coordinate with their respective RC HQ or their designated organization on all personnel and manpower matters such as, personnel staffing, performance, training, career progression, assignment rotation, etc.

E. **Training:** A trained force of DISA reservists and/or active-duty members (civilian and military) will provide initial mission orientation and training for the Elements.

1. Depending on the mission area, JRVIO personnel will be certified for the operational missions they are supporting. Certification programs are developed and administered by full time DISA personnel. The certifications are tailored to the mission area and geared to provide basic, advance, and expert level certification within the specific mission area. For example, reservists who have been trained on the Global Command and Control System Management Center "Hotline Desk" receive a Basic, Junior, or Senior Analyst certification depending on their skill level. They must have at least the Basic Analyst certification to assume the hotline desk weekend shift. Therefore, only personnel who have been trained and certified will be permitted to perform duties within their assigned operational areas. They will also be expected to continue information technology education through computer based training courses provided by DISA and other readily available alternatives.

2. As JRVIO personnel become familiar with DISA operations, they will be asked to perform special projects and/or participate in exercises. They will also be asked to provide training for newly hired reservists and to assist in the professional certification process. The objective of this professional diversity is to turn JRVIO personnel into "Cyber Warriors". The expectation is to have these "Cyber Warriors" trained and professionally certified to complement any of the DISA diverse missions.

3. Training of JRVIO members is the responsibility of the parent RC, in conjunction with the DISA Reserve Coordinator for those JRVIO elements in direct support of DISA and with the JTF-CND Commander for JRVIO assets in support of the JTF-CND.

Responsibilities:

A. **Military Services shall:**

1. Provide or make available RC personnel resources to DISA to staff the JRVIO on a full-time basis and part-time augmentation for specific tasks.
2. Realign manpower and funding from identified sources to the JRVIO with administrative control maintained by the parent RC Service.
3. Recruit and hire highly skilled personnel according to DISA mission requirements.
4. Fund all Reserve military personnel pay and allowances.
5. After initial mission orientation and training, ensure JRVIO element personnel maintain readiness posture as defined by Designed Operational Capability Statements.
6. Provide facilities for the JRVIO elements to perform their administrative functions

B. **Director, DISA shall:**

1. Serve as the Executive Agent for the JRVIO.
2. Provide the facilities and other administrative requirements to support the JRVIO, and/or establish any required Memorandum of Understanding for facility or administrative support with the DOD locations from which the JRVIO will operate.
3. Develop an implementation plan and Standard Operating Procedures (SOP).
4. When necessary, further support the JRVIO by capitalizing on existing DISA assigned RC personnel and identify, as appropriate, current and/or additional requirements.
5. Request necessary training and threat and vulnerability assessments support from Director, NSA.
6. Evaluate funding adequacy and support requirements for the JRVIO.
7. Assist Services during their recruitment processes by providing mission requirements such as, position and skill set descriptions.
8. Fund FTS positions.
9. Activate the JRVIO Management Cell.
10. Fund JRVIO element travel, per diem, equipment, and training expenses.
11. Provide the necessary facilities and equipment to train for and perform the DISA mission. The type of equipment (hardware and/or software) is dependent on the mission area supported).
12. Provide necessary initial and recurring training for the element personnel

C. **Commander, JRVIO shall:**

1. Provide for the technical proficiency and tactical competence of all assigned members.
2. Provide for the management of JRVIO training and exercises planning and coordination. Management includes the scheduling and coordination of training and exercises with DOD and other agencies.

D. ***The Director, NSA shall:***

1. Coordinate with ASD/C3I to ensure OPSEC, vulnerability analysis, threat assessment, and training support to the JRVIO as required.

E. **The Director, Joint Reserve Intelligence Program (JRIP) shall*:***

1. Coordinate with ASD/C3I to ensure OPSEC, vulnerability analysis, threat assessment, and training support to the JRVIO as required.

F. **ASD/C3I shall:**

1. Coordinate with the Director, NSA and the Director, JRIP to ensure OPSEC, vulnerability analysis, threat assessment, and training support to the JRVIO as required.

VI. **Organizational Stand-Up Timeline:** Initial operational capability will be within 18 months from the date of activation of the JRVIO, with full operational capability expected within 36 months from the date of activation. A prime objective is to establish a preliminary operational capability for the elements within 6 months of activation. However, this objective will be based on the JRVIO obtaining qualified personnel possessing strong information technology skills that meets the DISA mission requirements.

A. The functions listed below are required for the JRVIO to meet its responsibilities for initial operational capability.

1. Discovery of methods used to penetrate or disrupt computer systems and networks.
2. Analysis of tools and methods developed for use in CNA.
3. Perform computer system and network vulnerability assessment and penetrations.
4. Monitor Computer Emergency Response Team (CERT) Alerts, Warnings and Advisories.
5. Provide red/blue/white team assistance for joint exercises as requested.
6. Participate in joint training exercises to conduct CND.

7. Provide ongoing technical training to increase proficiency of assigned personnel.
8. Provide support to the JTF-CND.
9. Provide support to the GNOSC and RNOSCs.
10. Conduct IAVA Compliance Verification.

B. The functions listed below are required for the JRVIO to meet its responsibilities for full operational capability.

1. Develop contingency plans, tactics, techniques, and procedures to defend DOD computer systems and networks.
2. Evaluate whether appropriate action, risk assessment, and/or waivers are accomplished for noted discrepancies following standard procedures.
3. Coordinate with Defense-wide Information Assurance Program (DIAP) and Critical Asset Assurance Program (CAAP) authorities to ensure Service compliance with DOD Information Assurance (IA) policy and initiatives.
4. Provide JTF CND with Indications and Warnings of possible CNA based on information garnered during normal discovery activities.
5. Provide web log traffic analysis.
6. Provide staff augmentation to the JWRAC.

ADDENDUMS:

A. DISA RC Background Data:

DISA RC Support by Type	DISA Current RC Support	% of RC Supporting IO/IA Activities	% of RC IO/IA Support Operating Virtually	New RC IO/IA Billets from Upcoming JTMD/POM	% of New RC IO/IA Billets Operating Virtually[30]
Full-Time					
ARNG					
Officer					
Enlisted					
USAR					
Officer					
Enlisted					
ANG					
Officer					
Enlisted					
AFRC					
Officer	1			2	
Enlisted				10	
USNR					
Officer					
Enlisted	1				
USMCR					
Officer					
Enlisted					
Part-Time					
ARNG					
Officer	3			24	
Enlisted	5			12	
USAR					
Officer	12			28	
Enlisted	116			37	
ANG					
Officer	1			15	
Enlisted	2			33	
AFRC					
Officer	54			54	
Enlisted	21			211	
USNR					
Officer	3			13	
Enlisted	16			10	
USMCR					
Officer	7			9	
Enlisted	5			24	
Totals	**247**	**70%**	**85%**	**482**	**58.5%**
Totals Expressed as Numbers Derived From %	**247**	**175**	**150**	**482**	**282**

[30] For purposes of this study, all full-time support dedicated to enabling virtual operations is considered virtual for accounting purposes.

B. **DISA JRVIO:**

DISA JRVIO MANPOWER REQUIREMENTS STAFFING:

Full Time Support:		**FY01**	**FY02**	**FY03**	**FY04**	**FY05**	**FY06**
AFRC							
Enlisted		10	10	10	10	10	10
Drilling Reservists:							
ARNG							
Officer		27	27	27	27	27	27
Enlisted		17	17	17	17	17	17
USAR							
Officer		20	20	20	20	20	20
Enlisted		56	56	56	56	56	56
ANG							
Officer		16	16	16	16	16	16
Enlisted		35	35	35	35	35	35
AFRC							
Officer		22	22	22	22	22	22
Enlisted		213	213	213	213	213	213
USNR							
Officer		11	11	11	11	11	11
Enlisted							
USMCR							
Officer		5	5	5	5	5	5
Enlisted							
Total (Full-time + Part-time)		432	432	432	432	432	432

C. **RC Support from DISA Earmarked for JTF-CND:** Of the above numbers the following subset has been earmarked for JTF-CND support. These are not additional numbers, but rather duplicative of those referenced above.

Drilling Reservists:		**FY01**	**FY02**	**FY03**	**FY04**	**FY05**	**FY06**
ARNG							
Officer		16	16	16	16	16	16
Enlisted		10	10	10	10	10	10
USAR							
Officer		9	9	9	9	9	9
Enlisted		7	7	7	7	7	7
ANG							
Officer		6	6	6	6	6	6
Enlisted		3	3	3	3	3	3
AFRC							
Officer		17	17	17	17	17	17
Enlisted		19	19	19	19	19	19
USNR							
Officer		7	7	7	7	7	7
Enlisted							
USMCR							
Officer		4	4	4	4	4	4
Enlisted							
Total		**98**	**98**	**98**	**98**	**98**	**98**

D. **Resources:** The JRVIO will train and operate with hardware and software that are contained within the DISA Operation Centers/Commands. However, if additional equipment is required, the DISA JRP and Center/Command senior leadership will work together to acquire the necessary equipment to perform the missions. When feasible, JRVIO elements will co-locate with other RC Units at locations and facilities. This sharing of facilities will mitigate standing up new sites across the country.

E. **Security:** The nature of the different missions drives the security requirements. However, it is envisioned that JRVIO personnel may require a Top Secret/Special Compartmented Information (SCI) clearance. On a case-by-case basis, interim Top Secret clearances are allowed until the Top Secret/SCI status is achieved.

JRVIO Training Strategy

I. **BASIC TRAINING:** All accessions (Officer and Enlisted; AC & RC) would receive training in basic military skills as prescribed by their Services. This would include a briefing on IO that is standardized across the Services and based on Joint Pub 3-13.

II. **ADVANCED TRAINING:** All accessions being trained for specified IO skill identifiers would receive two modules of advanced training:

A. The first module would consist of a Joint training curriculum designed to cover , at a minimum:

1. IO doctrine and strategy from a joint perspective
2. Overview of the separate disciplines involved (i.e., CA, PSYOP, PA, IT, etc.)
3. Integration of the IO disciplines for effective coordination, planning and execution of IO
4. Discipline specific training. Strong consideration should be given to defining standards at the DOD level for IO disciplines that do not require significantly different skill sets from service to service. For example, Public Affairs Officers could be trained to the same curricula at a single school. Systems Administrators should be trained to the same standard including familiarity with all DOD operating systems, hardware platforms and software packages. (Note: Maximum, sensible standardization of these systems platforms and packages across the services would simplify this task). Consideration should also be given to use of curricula developed outside of DOD (academic, commercial, industrial) that meet DOD needs and can be delivered to a consistent standard at all DOD training venues.

B. The second module would consist of service specific requirements to produce a skill identifier to service standards:

1. Operation of service specific equipment
2. Service command, control and communication procedures
3. Service IO doctrine and strategy, with emphasis on the way it supports Joint doctrine and strategy
4. Additional discipline training (or OJT) to insure a service oriented knowledge base when serving in a service specific, non-IO related assignment

C. A common skill identifier could be used for the same discipline in all Services to indicate completion of a common course in these specific disciplines. This would allow for filling billets based on ability rather than Service.

III. **SUSTAINMENT:** All IO disciplines should be assigned a proponent to monitor currency of training modules:

A. The Services would be the proponents for Service specific modules.

B. Any appropriate Service or DOD entity could be designated the proponent for a discipline.

C. The proponent must maintain a "Change Level" system to account for modification to curricula.

D. The proponent must establish decision points to determine when the level of change to the curricula means that the knowledge level of previously trained personnel has degraded to an unacceptable level.

E. The proponent must then develop and deliver a training update to bring the entire field population of the discipline to the same standard.

IV. **CIVILIAN ACQUIRED SKILLS:** Civilian acquired skills (CAS) may derive from a knowledge and experience base or from a specific skill set that can be based on knowledge, experience and/or training. Where a skill can be easily tested for proficiency (i.e. language) or an accepted documentation of training can be provided, personnel can be credited with completion of equivalent training. Such accreditation and the mechanism to certify it would rest with the proponent of the discipline involved. In all other cases, DOD training must be accomplished and certified to allow award of a skill identifier.

V. **TRAINING DELIVERY:**

A. As training modules are developed, great attention must be given to modularization that would ease the burden of delivery to the RC. Where initial and follow-on training can be conducted in blocks of two weeks or less, the use of AT for training purposes by the RC is appropriate. Where the required training exceed two weeks in length and requires beginning-to-end delivery for maximum effectiveness, it must be formatted to allow for delivery during normal (or flexible) IDT.

B. One method for delivery to the RC might be computer based training (CBT). An individual could access a web site at their own pace to obtain training. To make this an option that would be pursued in a timely fashion and not detract form other IDT evolutions, a stipend for successful completion might be offered in addition to normal drill pay.

C. Alternately, DOD might fund a tuition reimbursement program for individuals taking a civilian course of study that can be directly equated to a portion of their required discipline training. (This could be used as a recruiting and retention incentive.)

Acronyms

AAG	Analysis and Assessment Group
AC	Active Component
ACTD	Advanced Concept Technology Demonstration
ADCON	Administrative Control
ADL	Advanced Distributed Learning
ADSW	Active Duty Special Work
ADT	Active Duty for Training
AFSC	Air Force Skill Code
AGR/TAR	Active Guard and Reserve/Training and Administration of Reserves
AOR	Area of Operations
ASD(C3I)	Assistant Secretary of Defense for Command, Control, Communications and Intelligence
ASD/RA	Assistant Secretary of Defense for Reserve Affairs
AT	Annual Training
ATG	Advance Technology Group
BDA	Battle Damage Assessment
C/S/A	CINCs/Services/Agencies
C2	Command and Control
C2W	Command and Control Warfare
C3I	Command, Control, Communications and Intelligence
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CBT	Computer Based Training
CCG	Community Coordination Group
CERT	Computer Emergency Response Team
CINC	Commander In Chief
CIO	Chief Information Officer
CNA	Computer Network Attack
CND	Computer Network Defense
CNO	Computer Network Operations
COMSEC	Communications Security
CONOPS	Concept of Operations
CONPLAN	Concept Plans
CONUS	Continental United States
CWE	Collaborative Workspace Environment

CVW	Collaborative Virtual Workspace
DCI	Director Central Intelligence
DCIS	Defense Criminal Investigative Service
DEPSECDEF	Deputy Secretary of Defense
DIA	Defense Intelligence Agency
DIO	Defense Information Operations
DIRNSA	Director, National Security Agency
DISA	Defense Information System Agency
DOD	Department of Defense
DPG	Defense Planning Guidance
DSL	
DSS	Defense Security Services
EW	Electronic Warfare
FOC	Full Operating Capability
FTS	Full-Time Support
FY	Fiscal Year
FYDP	Future Years Defense Program
GNOSC	Global Network Operations and Security Center
IA	Information Assurance
IAVA	Information Assurance Verification Assistance
IDT	Inactive Duty Training
ILRP	Interim Long Range Plan
INFOSEC	Information Systems Security
IO	Information Operations
IOC	Interim Operating Capability
IO-D	Defensive Information Operations
IO-O	Offensive Information Operations
IOTC	Information Operations Technology Center
ISP	Internet Service Provider
IT	Information Technology
IT	Individual Training
IWS	Information Workspace
JBC	Joint C4ISR Battle Center
JCMA	Joint COMSEC Monitoring Activity
JCMAT	Joint COMSEC Monitoring and Analysis Team
JCS	Joint Chiefs of Staff
JIC	Joint Intelligence Center
JIOC	Joint Information Operations Center (Formerly JC2WC)

JRIC	Joint Reserve Intelligence Center
JRIP	Joint Reserve Intelligence Program
JRVIO	Joint Reserve Component Virtual Organization for Information Operations
JS	Joint Staff
JTF	Joint Task Force
JTF-CND	Joint Task Force-Computer Network Defense (USSPACECOM)
JTMD	Joint Table of Manpower Distribution
JWCA	Joint Warfighting Capabilities Assessment
JWAC	Joint Warfighting Analysis Center
JWFC	Joint Warfighting Center
JWICS	Joint Worldwide Intelligence Communications Systems
LAN	Local Area Network
LOAC	Law of Armed Conflict
LRP	Long Range Plan
MOE	Measures of Effectiveness
MOS	Military Occupational Specialty
MOU	Memorandum of Understanding
MLS	Multi-Level Security
MTT	Mobile Training Team
MTW	Major Theater War
NEC	Naval Enlisted Classification
NC	North Carolina
NG	National Guard
NOSC	Network Operations and Security Center
NRSG	Naval Reserve Security Group
NSA	National Security Agency
NSOC	National Security Operations Center
O&M	Operations and Maintenance
OACJCS/NG&RM	Office of the Assistants to the Chairman of the Joint Chiefs of Staff for National Guard and Reserve Matters
OASD(C3I)	Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
OASD-RA	Office of the Assistant Secretary of Defense for Reserve Affairs
OPFOR	Opposing Forces
OPSEC	Operations Security
OPTEMPO	Operations Tempo
OSD	Office of the Secretary of Defense

OSIS	Open Source Information System
PBD	Program Budget Decision
PKI	Public Key Infrastructure
PPBS	Planning, Programming and Budget System
PoC	Proof of Concept
POG	Psychological Operations Group
POM	Program Objective Memorandum
POP	Point of Presence
PSYOP	Psychological Operations
RA	Reserve Affairs
RACI	Rapid Access to Information Operations Information
RC	Reserve Component
RCE-05	Reserve Component Employment 2005 Study
RCMC	Regional COMSEC Monitoring Center
RNOSC	Regional Network Operations and Security Centers
ROE	Rules of Engagement
ROTC	Reserve Officer Training Corps
RSOI	Reception, Staging, and Onward Integration
SCI	Sensitive Compartmented Information
SECDEF	Secretary of Defense
SIPRNET	Secure Internet Protocol Router Network
SME	Subject Matter Expert
SOF	Special Operations Forces
SOP	Standing Operating Procedures
SSC	Smaller-Scale Contingencies
SSG	Senior Steering Group
STO	Special Technical Operations
SVC	Switched Virtual Circuits
SYNOP	Synergized Prototypes
TEP	Theater Engagement Plans
TS/SCI	Top Secret/Special Compartmented Information
TTP	Tactics, Techniques, and Procedures
TV	Television
UCMJ	Uniform Code of Military Justice
UCP	Unified Command Plan
UE	Unified Endeavor
UFL	ULCHI FOCUS LENS
US	United States

USAFR	US Air Force Reserve
USAR	US Army Reserve
USEUCOM	United States European Command
USCENTCOM	United States Central Command
USPACOM	United States Pacific Command
USJFC OM	United States Joint Forces Command
USG	United States Government
USMCR	Marine Corps Reserve
USNR	US Navy Reserve
USSOCOM	United States Special Operations Command
USSTRATCOM	United States Strategic Command
USSOUTHCOM	United States Southern Command
USSPACECOM	US Space Command
VPN	Virtual Private Network
VTC	Video Teleconference
WAN	Wide Area Network
WBIL	Worldwide Basic Information Library

Glossary

Access Control – Process of granting access to information system resources only to authorized users, programs, processes, or other systems. [NSTISSI 4009, 1996]

Accountability – 1. (COMSEC) Principle that an individual is entrusted to safeguard and control equipment, keying material, and information and is answerable to proper authority for the loss or misuse of that equipment or information; 2. (Information Systems) Property that allows auditing of information system activities to be traced to persons or processes that may then be held responsible for their actions. [NSTISSI 4009, 1996]

Accreditation – Formal declaration by a Designated Approving Authority (DAA) that an information system (IS) is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. [NSTISSI 4009, 1999]

Advanced Intelligent Network (AIN) – A proposed intelligent-network (IN) architecture that includes both IN/1+ and IN/2 concepts. [Federal Standard 1037C]

Assurance – 1. In the context of CAAP, assurance is a process of identifying assets deemed critical to the Department of Defense in peacetime, crisis and war; assessing the potential threats to these assets and the capabilities they provide; quantifying the likely non-availability to the Department of Defense under various hazard scenarios; identifying potential actions that can be taken to restore those assets (or functionality they provide) if they are lost, damaged, corrupted, or compromised; and identifying and recommending options to protect, mitigate, and improve the availability of these Critical Assets to the DOD organizations that own, use, and control them. It includes a range of activities to systematically inform planners and decision makers of the probability of availability and quality (e.g., integrity, reliability, confidentiality, survivability, endurance, capacity, adequacy) of specific assets or services under given scenarios; quantifying the likely impact of non-availability to the military operation or defense activity; and identifying and prioritizing options to improve the likelihood of the availability of specific assets or services in specific scenarios. Examples of assurance activities that can improve the likelihood of asset availability include protection (preventing, by whatever means, the disruption or corruption of an asset); mitigation or moderation of the effects of disruption or corruption (by controlling the damage, providing alternative services, and reducing demand on the asset); and planning for and providing timely restoration or recovery. Alternatively, plans can be made to absorb the loss of otherwise anticipated services. Assurance of a Critical Asset is the responsibility of the owning or controlling DOD Component. [DODD 5160.4]; 2. A measure of confidence that the security features and architecture of an AIS accurately mediate and enforce the security policy. If the security features of AIS are relied on to protect classified or sensitive unclassified information and restrict user access, the features must be tested to ensure that the security policy is enforced and may not be circumvented during AIS operation. [DODD 5200.28, 1988]

Asynchronous Communications – A transmission method in which each transmitted data character is preceded by a start bit and followed by a stop bit. Permits time intervals between each character to vary. [Pfaffenberger, Brian, PhD, *Que's Computer User's Dictionary*, 1990; Unified INFOSEC Glossary, Aug 1999]

Attack – The intentional act of attempting to bypass security controls on an Automated Information System. [JIWG Proposed Common Terminology]

Attack Assessment – An evaluation of information to determine the potential or actual nature and objectives of an attack for the purpose of providing information for timely decisions. [Joint Pub 1-02, 1994]

Audit – Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. [NSTISSI No. 4009, 1999]

Authenticate – To verify the identity of a user, user device, or other entity, or the integrity of data stored, transmitted, or otherwise exposed to unauthorized modification in an information system, or to establish the validity of a transmission. [NSTISSI 4009, 1996]

Automated Information System Security – Measures and controls that protect AIS against denial of service and unauthorized (accidental or intentional) disclosure, modification, or destruction of AISs and data. AIS security includes consideration of all hardware and/or software functions, characteristics and/or features; operational procedures, accountability procedures, and access controls at the central computer facility, remote computer, and terminal facilities; management constraints; physical structures and devices; and personnel and communication controls needed to provide an acceptable level of risk for the AIS and for the data and information contained in the AIS. It includes the totality of security safeguards needed to provide an acceptable protection level for AIS and for data handled by AIS. [NCSC TG-004]

Automated Systems Security Incident Support Team (ASSIST) – An integrated DOD operational response capability for handling information systems security incidents, attacks and threats to DOD-interest automated telecommunications systems. ASSIST provides telephonic, on-line, and on-site support 24 hours a day, 7 days a week, 52 weeks a year. [http://www.fas.org/irp/congress/1996_hr/s960605a.htm]

Availability – Ensuring that data transmission or computing processing systems are not denied to authorized users. [CJCSI 6510.01B, 1997]

Availability of Services – Timely, reliable access to data and information services for authorized users. [NSTISSI 4009, 1996]

Certificate Authority Workstation (CAW) – Commercial-off-the-shelf (COTS) workstation with a trusted operating system and special purpose application software that is used to issue certificates. [NSTISSI No. 4009, 1999]

Certification – Comprehensive evaluation of the technical and non-technical security features of an IS and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements. [NSTISSI No. 4009, 1999]

Certification Authority (CA) – Third level of the Public Key Infrastructure (PKI) Certification Management Authority responsible for issuing and revoking user certificates, and exacting compliance to the PKI policy as defined by the parent Policy Creation Authority (PCA). [NSTISSI No. 4009, 1999]

Classified National Security Information – Information that has been determined pursuant to Executive Order 12958 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form. [Executive Order 12958, 1995]

Client-Server Architecture – Any network-based software system that uses client software to request a specific service, and corresponding server software to provide the service from another computer on the network. [FS -1037C, 1966]

Collaborative Workspace Environment – An automation environment that enables people to converse, collaborate, and interact regardless of geographic location. The workspace establishes and manages a collection of virtual rooms with each incorporating the people, information, and tools appropriate to a task, operation, or service. Users can move from room to room just as they would in a building, meeting team members, discovering collaborators, sharing knowledge, and performing functions as they would if physically collocated. [ASD/RA derived]

Combatant Command – A unified or specified command with a broad continuing mission under a single commander established and so designated by the President, through the Secretary of Defense and with the advice and assistance of the Chairman of the Joint Chiefs of Staff. Combatant commands typically have geographic or functional responsibilities. [JP 1-02]

Command and Control-Protect (C2-Protect) – The maintenance of effective C2 of own forces by turning to friendly advantage or negating adversary efforts to deny information to, influence, degrade, or destroy the friendly C2 system. C2-Protect can be offensive or defensive in nature. Offensive C2-Protect uses the five elements of C2W to reduce the adversary's ability to conduct C2-attack. Defensive C2-Protect reduces friendly C2 vulnerabilities to adversary C2-attack by employment of adequate physical, electronic, and intelligence protection. [Field Manual 100-6 (adapted from CJCSI 3210.03), 1996]

Command and Control Warfare (C2W) – The integrated use of operations security (OPSEC), military deception, psychological operations (PSYOP), electronic warfare (EW) and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade or destroy adversary C2 capabilities, while protecting friendly C2 capabilities against such actions. Command and Control Warfare applies across the operational continuum and all levels of conflict. C2W is both offensive and defensive. [JP1-02, 1994]; NOTE: In Joint Pub 1-02, 1994, this definition of C2W is a replacement for Command, Control, and Communications Countermeasures.

a. **Counter-C2** – To prevent effective C2 of adversary forces by denying information to, influencing, degrading, or destroying the adversary C2 system.

b. **C2-Protection** – To maintain effective command and control of own forces by turning to friendly advantage or negating adversary efforts to deny information to, influence, degrade, or destroy the friendly C2 system.

Command, Control, Communications, and Computer (C4) Systems – Integrated systems of doctrine, procedures, organizational structures, personnel, equipment, facilities, and communications designed to support a commander's exercise of command and control through all phases of the operational continuum. [JP-02, 1994]

Commercial-off-the-shelf (COTS) – An item of hardware or software that has been produced by a contractor and is available for general purchase. Such items are at the unit level or higher. Further, such items must have meaningful reliability, maintainability, and logistics historical data. [DISA, TAFIM, 1997]

Common Operating Environment – The collection of standards, specifications, and guidelines, architecture definitions, software infrastructures, reusable components, application programming interfaces (APIs), methodology, runtime environment definitions, reference implementations, and methodology, that establishes an environment on which a system can be built. The COE is the vehicle that assures interoperability through a reference implementation that provides identical implementation of common functions. It is important to realize that the COE is both a standard and an actual product. [DII COE I&RTS]

Communications Security (COMSEC) – Measures and controls taken to deny unauthorized persons information derived from telecommunications and ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material. [NSTISSI 4009, 1996]

Computer Emergency Response Team (CERT) – An organization chartered by an information system owner to coordinate and/or accomplish necessary actions in response to computer emergency incidents that threaten the availability or integrity of its information systems. [DODD 5160.54]

Computer Intrusion – An incident of unauthorized access to data or an Automated Information System. [JIWG]

Computer Security – Measures and controls that ensure confidentiality, integrity, and availability of IS assets including hardware, software, firmware, and information being processed, stored, and communicated. [NSTISSI No. 4009, 1999]

Concept of Operations (CONOP) – Document detailing the method, act, process, or effect of using an IS. [NSTISSI No. 4009, 1999]

Counterdeception – Negating. neutralizing, or diminishing the effects of or advantage from foreign deception operations. [Joint Pub 1-02, 1994]

Critical Asset – Any facility, equipment, service, or resource considered essential to DOD operations in peace, crisis, and war and warranting measures and precautions to ensure its continued efficient operation, protection from disruption, degradation or destruction, and timely restoration. Critical assets may be DOD assets or other government or private assets, (e.g., Industrial or Infrastructure Critical Assets), domestic or foreign, whose disruption or loss would render DOD Critical Assets ineffective or otherwise seriously disrupt DOD operations. Critical assets include both traditional "physical" facilities and/or equipment, non-physical assets (such as software systems) or "assets" that are distributed in nature (such as command and control networks, wide area networks or similar computer-based networks). [DODD 5160.54, Jan. 1998]

Critical Infrastructures – Certain national infrastructures so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States. These critical infrastructures include telecommunications, electrical power systems, gas and

oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire and rescue), and continuity of government. [Executive Order 13010]

Criticality – A measure of how important the correct and uninterrupted functioning of the system is to national security, human life, safety, or the mission of the using organization; the degree to which the system performs critical processing. [SABI Handbook]

Cryptography – Art or science concerning the principles, means, and methods for rendering plain information unintelligible and of restoring encrypted information to intelligible form. [NSTISSI 4009, 1996]

Damage Assessment – 1. The determination of the effect of attacks on targets. (DOD); 2. A determination of the effect of a compromise of classified information on national security. [Joint Pub 1-02, 1994]

Damage to the National Security – Harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, to include the sensitivity, value, and utility of that information. [Executive Order 12958, 1995]

Data – Representation of facts, concepts, or instructions in a formalized manner suitable for communications, interpretation, or processing by humans by automatic means. Any representations such as characters or analog quantities to which meaning is, or might be, assigned. [Joint Pub 1-02, 1994]

Data Encryption Standard (DES) – Cryptographic algorithm, designed for the protection of unclassified data and published by the National Institute of Standards and Technology in Federal Information Processing Standard (FIPS) Publication 46. [NSTISSI No. 4009, 1999]

Defense in Depth – The security approach whereby layers of IA solutions are used to establish an adequate IA posture. Implementation of this strategy also recognizes that, due to the highly interactive nature of the various systems and networks, IA solutions must be considered within the context of the shared risk environment and that any single system cannot be adequately secured unless all interconnected systems are adequately secured. [DEPSECDEF Policy Memo 6-8510]

Defense Information Infrastructure (DII) – The DII encompasses information transfer and processing resources, including information and data storage, manipulation, retrieval, and display. More specifically, the DII is the shared or interconnected system of computers, communications, data, applications, security, people, training, and other support structure, serving the DOD's local and worldwide information needs. The DII connects DOD mission support, command and control, and intelligence computers and users through voice, data, imagery, video, and multimedia services, and also provides information processing and value-added services to subscribers over the DISN. Unique user data, information, and user applications are not considered part of the DII. [ASD (C3I) Memo, 1994]

Defense Information Systems Network (DISN) – 1. A sub-element of the DII, the DISN is the DOD's consolidated worldwide enterprise level telecommunications infrastructure that provides the end-to-end information transfer network for supporting military operations. It is transparent to its users, facilitates the management of information resources, and is responsive to national security

and defense needs under all conditions in the most efficient manner. [DODI 5200.40, DITSCAP, modified; ASD (C3I) Memo, 1994]; 2. The DISN is an information transfer network with value-added services for supporting national defense C3I decision support requirements and CIM functional business areas. As an information transfer utility, the DISN provides dedicated point-to-point, switched voice and data, imagery and video teleconferencing communications services. [CJCSI 6211.02, 1993]

Defense Infrastructure – Infrastructure owned, operated or provided by the Department of Defense. Defense Infrastructure Sectors include the DII, C3, Space, ISR, Financial Services, Logistics, Public Works (includes DOD-owned or -operated utilities, roads, rails and railheads and their interface to commercial and other Government systems), Personnel, Health Affairs and Emergency Preparedness. [Modified from DODD 5160.54]

Defense Switched Network – Component of the Defense Communications System that handles Department of Defense voice, data, and video communications. [http://call.army.mil/call/thesaur/index.htm]

Defensive Information Operations – The defensive IO process integrates and coordinates polices and procedures, operations, personnel, and technology to protect information and to defend information systems. Defensive IO are conducted through information assurance, physical security, operations security, counter deception, counter psychological operations, counter intelligence, electronic protect, and special information operations. Defensive IO objectives ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and systems for their own purposes. [CJCSI 6510.01B, 1997]

Denial of Service – Action or actions that result in the inability of an AIS or any essential part to perform its designated mission, either by loss or degradation of operational capability. [DODD 5200.28, 1988]

DOD Information Technology Security Certification and Accreditation Process (DITSCAP) – The standard DOD approach for identifying information security requirements, providing security solutions, and managing information technology system security. [DODI 5200.40]

DOD Installation – A facility subject to the custody, jurisdiction, or administration of any DOD Component. This term includes, but is not limited to, military reservations, installations, bases, posts, camps, stations, arsenals, or laboratories where a DOD Component has operational responsibility for facility security and defense. Examples are facilities where the military commander or other specified DOD official under provisions of DOD Directive 5200.8 has issued orders or regulations for protection and security. Both industrial assets and infrastructure assets, not owned by the Department of Defense, may exist within the boundaries of a military installation. [DODD 5160.54]

Domain Name Servers – Servers that retain the addresses and routing information for TCP/IP LAN users. [Federal Standard 1037C]

Electronic Data Interchange – The sending, transmission, reception, and interchange of information and data relating to business transactions via electronic means. EDI is analogous to EFT (Electronics Funds Transfer) but it is more complicated to establish standards for EDI, as each organization typically has its own document formats and its own ordering and invoice practices.

Establishing an EDI service involves devising a standard format for each type of transaction that suits all participants. EDI has developed from pioneer work initially in the United Kingdom and later the rest of Europe and the USA. [http://call.army.mil/call/thesaur/index.htm]

Electronic Warfare (EW) – Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. The three major subdivisions within electronic warfare are: electronic attack, electronic protection, and electronic warfare support. [Joint Pub 1-02, 1994]

Encryption – Process of transforming data into an unintelligible form to conceal its meaning. [USAF Manual 33-270]

External Certificate Authority (ECA) – An agent that is trusted and authorized to issue certificates to approved vendors and contractors for the purpose of enabling secure interoperability with DOD entities. Operating requirements for ECAs must be approved by the DOD CIO, in coordination with the DOD Comptroller and the DOD General Counsel. [DOD PKI Policy]

Firewall – A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria. [PC Webopaedia, 1997]

Force Protection – Security program developed to protect Service members, civilian employees, family members, facilities and equipment, in all locations and situations, accomplished through planned and integrated application of combating terrorism, physical security, operations security, personal protective services supported by intelligence, counterintelligence, and other security programs. [Draft DODD 2000.12]

Function – Appropriate or assigned responsibility, mission, task, power, or duty of an individual, office, or organization. A functional area (e.g., personnel) comprises of one or more functional activities (e.g., recruiting), each of which consists of one or more functional processes (e.g., interviews). [Joint Pub 1-02, 1994]

Global Information Infrastructure (GII) – Includes the information systems of all countries, international and multinational organizations and multi-international commercial communications services. [CJCSI 6510.01B, 1997]

Government Services Information Infrastructure (GSII) – The U.S. Government information infrastructure portion of the National Information Infrastructure (NII) used to link people to government and its services. Sometimes referred to as Government Information Technology Services (GITS). [GITS document, Chapter A-15]

Identification and Authentication – Verification of the originator of a transaction, similar to the signature on a check or a Personal Identification Number (PIN) on a bankcard. [CJCSI 6510.01B, 1997]

Incident and Detection Response Capabilities – The establishment of mechanisms and procedures to monitor information systems and networks; detect, report and document attempted or

realized penetrations of those systems and networks; and institute appropriate countermeasures or corrective actions. [DEPSECDEF Policy Memo 6-8510]

Indications and Warning – Those are intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that could involve a threat to the United States or allied military, political, or economic interests or to U.S. citizens abroad. It includes forewarning of enemy actions or intentions; the imminence of hostilities; insurgency; nuclear/non-nuclear attack on the United States, its overseas forces, or allied nations; hostile reactions to United States reconnaissance activities; terrorist attacks; and other similar events. [Joint Pub 1-02, 1994]

Information – 1. Facts, data, or instructions in any medium or form. [DODD S-3600.1, 1996]; 2. The meaning that a human assigns to data by means of the known conventions used in their representation. [Joint Pub 1-02, 1994]; 3. Any communication or representation of knowledge such as facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms. [DISA, TAFIM, 1997; OMB Circ A-130, 1996]

Information Assurance – Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. [DODD S-3600.1, 1996]

Information Assurance Vulnerability Alert (IAVA) – The comprehensive distribution process for notifying CINC's, Services and agencies (C/S/A) about vulnerability alerts and countermeasures information. The IAVA process requires C/S/A receipt acknowledgment and provides specific time parameters for implementing appropriate countermeasures depending on the criticality of the vulnerability. [JTF-CND CONOP]

Information Environment – the aggregate of individuals, organizations, or systems that collect, process, or disseminate information, including the information itself. [Joint Pub 3-13, 1998]

Information Integrity – The state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed.
[Executive Order 12958, 1995]

Information Operations (IO) – 1. Actions taken to affect adversary information and Information Systems (IS) while defending one's own information and ISs. [Joint Pub 3-13, 1998; NSTISSI No. 4009, 1999]; 2. The combination of four functional activities: electronic warfare, computer network operations, information protection, and perception management. [ASD/C3I White Paper, DOD Concept for Information Operations]

Information Operations Condition (INFOCON) – The INFOCON is a comprehensive defense posture and response based on the status of information systems, military operations, and intelligence assessments of adversary capabilities and intent. The INFOCON system presents a structured, coordinated approach to defend against a computer network attack. INFOCON measures focus on computer network-based protective measures. Each level reflects a defensive posture based on the risk of impact to military operations through the intentional disruption of friendly information systems. INFOCON levels are: NORMAL (normal activity); ALPHA (increased risk of attack); BRAVO (specific risk of attack); CHARLIE (limited attack); and DELTA

(general attack). Countermeasures at each level include preventive actions, actions taken during an attack, and damage control/mitigating actions. [CJCS Memo CM-510-00, 10 March 1999]

Information Operations Technical Center (IOTC) – An organization housed at NSA but staffed by IT experts from across DOD and government agencies in support of Services, Unified Commands, and National requirements. [ASD/RA derived explanation]

Information Security – The protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional. [FS -1037C, 1996]

Information Superiority – 1. That degree of dominance in the information domain which permits the conduct of operations without effective opposition. [DODD S-3600.1, 1996]; 2. The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary to do the same. [Joint Pub 3-13, 1998]

Information System – 1. The entire infrastructure, organization, personnel and components for the collection, processing, storage, transmission, display, dissemination and disposition of information. [NSTISSI 4009]; 2. The organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual. In information warfare, this includes the entire infrastructure, organizations, and components that collect, process, store, transmit, display, and disseminate information. [DODD S-3600.1, 1996]

Information Systems Security – The protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users or the provision of service to unauthorized users (includes those measures necessary to detect, document, and counter such threats). [NSTISSI 4009, 1996]

Information Warfare (IW) – Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries. [DODD S-3600.1, 1996]

Infrastructure – The framework of interdependent networks and systems comprising identifiable industries, institutions, and distribution capabilities that provide a continual flow of goods and services essential to the defense and economic security of the United States, to the smooth functioning of governments at all levels, and to society as a whole. [CIWG, Report: Options; DODD 5160.54, Critical Asset Assurance Program - CAAP]

Infrastructure Analysis and Assessment – Coordinated identification of DOD, National Defense Infrastructure, and International Defense Infrastructure critical assets, their system and infrastructure configuration and characteristics, and the interrelationships among infrastructure sectors; assessment of their vulnerabilities; quantification of the relationship between military plans and operations and critical assets / infrastructures; and assessment of the operational impact of loss or compromise. [CIP Working Definition]

Infrastructure Asset – Any infrastructure facility, equipment, service or resource that supports a DOD Component. A Critical Infrastructure Asset is an infrastructure asset deemed essential to DOD operations or the functioning of a Critical Asset. [DODD 5160.54]

Infrastructure Assurance – The surety of readiness, reliability, and continuity of infrastructures such that they are: (1) less vulnerable to disruptions or attack; (2) harmed to a lesser degree in the event of a disruption or attack; and (3) can be readily reconstituted to reestablish vital capabilities. [CIWG, Report: Options]

Integrity – Absolute verification that data has not been modified in transmission or during computer processing. [CJCSI 6510.01B, 1997]

Intelligence Community Information – Refers to Sensitive Compartmented Information and any other information that is classified pursuant to section 1.5(c) of Executive Order 12958 that also bears special intelligence handling markings found in the "Authorized Classification and Control Markings Registry" maintained by the Community Management Staff. [DEPSECDEF Policy Memo 6-8510]

Intelligence Estimate – The appraisal, expressed in writing or orally, of available intelligence relating to a specific situation or condition with a view to determining the courses of action open to the enemy or potential enemy and the order of probability of their adoption. [Joint Pub 1-02, 1994]

International Defense Infrastructure (IDI) – Those elements of international infrastructure that are critical to Department of Defense operations. [CIP Working Definition]

Interoperability – The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users. The degree of interoperability should be defined when referring to specific cases. [Joint Pub 1-02, 1994]

Local Area Network (LAN) – A data communications system that lies within a limited spatial area, has a specific user group, has a specific topology, and is not a public switched telecommunications network, but may be connected to one. (Note: LANs are usually restricted to relatively small areas, such as rooms, buildings, ships, and aircraft. An interconnection of LANs within a limited geographical area, such as a military base, is commonly referred to as a campus area network. An interconnection of LANs over a citywide geographical area is commonly called a metropolitan area network (MAN). An interconnection of LANs over large geographical areas, such as nationwide, is commonly called a wide area network (WAN). LANs are not subject to public telecommunications regulations. [FS -1037C, 1996]

Multiple Security Level/Multilevel Security (MLS) – Concept of processing information with different classifications and categories that simultaneously permits access by users with different security clearances and denies access to users who lack authorization. [NSTISSI No. 4009, 1999]

National Defense Infrastructure – Those assets in the other government and national infrastructure sectors and industrial assets that are critical to National Defense. [CIP Working Definition]

National Information Infrastructure (NII) – 1. The nation-wide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. The national information infrastructure encompasses a wide range of equipment, including: cameras, scanners, keyboards, facsimile machines, computers,

switches, compact disks, video and audio tape, cable, wire, satellites, fiber optic transmission lines, networks of all types, televisions, monitors, printers, and much more. The friendly and adversary personnel who make decisions and handle the transmitted information constitute a critical component of the national information infrastructure. [Joint Pub 3-13, Draft, 1997]; 2. System of high-speed telecommunications networks, databases, and advanced computer systems that will make electronic information widely available and accessible. The NII is being designed, built, owned, operated, and used by the private sector. In addition, the government is a significant user of the NII. The NII includes the Internet, the public switched network, and cable, wireless, and satellite communications. It includes public and private networks. As these networks become more interconnected, individuals, organizations, and governments will use the NII to engage in multimedia communications, buy and sell goods electronically, share information holdings, and receive government services and benefits. [IITF, NII Security: The Federal Role, 1995]

National Infrastructure – Those infrastructures essential to the functioning of the nation and whose incapacity or destruction would have a debilitating regional or national impact. National infrastructures include telecommunications, electrical power systems, gas and oil transportation and storage, water supply systems, banking and finance, transportation, emergency services, and continuity of government operations. [DODD 5160.54]

National Security Systems – Those telecommunications and information systems operated by the U.S. Government, its contractors, or agents, that contain classified information or, as set forth in 10 USC Section 2315, that involve intelligence activities, involve cryptologic activities related to national security, involve command and control of military forces, involve equipment that is an integral part of a weapon or weapon system, or involve equipment that is critical to the direct fulfillment of military or intelligence missions. [NSD-42, 1990]

Offensive Information Operations – The integrated use of assigned and supporting capabilities and processes, mutually supported by intelligence, to affect information and information systems to achieve or promote specific objectives. These capabilities and processes include, but are not limited to, operations security, military deception, psychological operations, electronic warfare, and physical destruction. [Joint Pub 3-13, Draft, 1997]

Open System – 1. A system that implements sufficient open specifications for interfaces, services, and supporting formats to enable properly engineered applications software: (a) to be ported with minimal changes across a wide range of systems, (b) to interoperate with other applications on local and remote systems, and (c) to interact with users in a style that facilitates user portability. [PCCIP]; 2. A system with characteristics that comply with specified, publicly maintained, readily available standards and that therefore can be connected to other systems that comply with these same standards. [FS -1037C, 1996]

Open Systems Environment (OSE) – The comprehensive set of interfaces, services, and supporting formats, plus user aspects for interoperability or for portability of applications, data, or people, as specified by information technology standards and profiles. [TAFIM, 1997]

Operations Security (OPSEC) – A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: (a) identify those actions that can be observed by adversary intelligence systems, (b) Determine indicators adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries, and (c) select and execute measures that eliminate or

reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. [Joint Pub 1-02, 1994]

Public Key Infrastructure (PKI) – 1. Framework established to issue, maintain, and revoke public key certificates accommodating a variety of security technologies, including the use of software. [NSTISSI No. 4009, 1999]**;** 2. An enterprise-wide service that supports digital signatures and other public key-based security mechanisms for DOD functional domain programs, including generation, production, distribution, control and accounting of public key certificates. [DEPSECDEF Policy Memo 6-8510]

Public Switched Network (PSN) – Any common carrier network that provides circuit switching among public users. Note: The term is usually applied to public switched telephone networks, but it could be applied more generally to other switched networks, e.g., packet-switched public data networks. [Federal Standard 1037C]

Precedence – A designation assigned to a message by the originator to indicate to communications personnel the relative order of handling and to the addressee the order in which the message is to be noted. [Joint Pub 1-02, 1994]

Protocol – 1. Set of rules and formats, semantic and syntactic, that permits entities to exchange information. [NSTISSI 4009, 1996]; 2. A formal set of conventions governing the format and control of interaction among communicating functional units. Protocols may govern portions of a network, types of service, or administrative procedures. For example, a data link protocol is the specification of methods whereby data communications over a data link are performed in terms of the particular transmission mode, control procedures, and recovery procedures. In layered communications system architecture, a formal set of procedures that are adopted to facilitate functional interoperation within the layered hierarchy. [FS -1037C, 1996]

Psychological Operations (PSYOP) – Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning and, ultimately, the behavior of foreign governments, organizations, groups, and individuals. The purpose of PSYOP is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. (PSYOP are a vital part of the broad range of U.S. political, military, economic, and informational activities. When properly employed, PSYOP can lower the morale and reduce the efficiency of enemy forces and could create dissidence and disaffection within their ranks.) [Joint Pub 3-53, 1993]

Readiness – Ability of forces, units, and weapon systems to deliver the designed output. [http://call.army.mil/call/thesaur/index.htm]

Reconstitution – Owner/operator directed restoration of critical assets and/or infrastructure. [DOD CIPP]

Reliability – 1. The ability of an item to perform a required function under stated conditions for a specified period of time. 2. The probability that a functional unit will perform its required function for a specified interval under stated conditions. 3. The continuous availability of communication services to the general public, and emergency response activities in particular, during normal operating conditions and under emergency circumstances with minimal disruption. [Federal Standard 1037C]

Response – Coordinated third party (not owner/operator) emergency (e.g., medical, fire, hazardous or explosive material handling), law enforcement, investigation, defense, or other crisis management service aimed at the source or cause of the incident. [CIP Working Definition]

Risk – The probability that a particular threat will exploit a particular vulnerability of the system. [NSA, NCSC Glossary, 1988]

Risk Analysis – The process of identifying security risks, determining their magnitudes, and identifying areas needing safeguards. Risk analysis is a part of risk management. Synonymous with risk assessment. [NSA, NCSC Glossary, 1988]

Risk Assessment – Process of analyzing threats to and vulnerabilities of an information system, and the potential impact that the loss of information or capabilities of a system would have on national security and using the analysis as a basis for identifying appropriate and cost-effective counter-measures. Synonymous with risk analysis. [NSTISSI No. 4009, 1996]

Risk Management – The total process of identification, measurement, control, and minimization of security risks in information systems to a level commensurate with the value of the assets protected. [NSTISSI No. 4009, 1996]

Secret and Below Interoperability (SABI) Initiative – An ASD (C3I) directed, JCS sponsored, NSA/DISA executed initiative to enhance Secret and Below Interoperability, measure community risk, and protect the DOD information systems infrastructure. [SABI Handbook)]

Security Management – In network management, the set of functions: (1) that protects telecommunications networks and systems from unauthorized access by persons, acts, or influences, and (2) that includes many sub-functions, such as creating, deleting, and controlling security services and mechanisms; distributing security-relevant information; reporting security -relevant events; controlling the distribution of cryptographic keying material; and authorizing subscriber access, rights, and privileges. [Federal Standard 1037C]

Security Measures (Metrics) – Elements of software, firmware, hardware, or procedures that are included in a system for the satisfaction of security specifications. [NCSC TG-004]

Security Policies – A set of rules and procedures regulating the use of information including its processing, storage, distribution, and presentation. [Working Group 3N102, Joint Technical Committee/Subcommittee 27/N734]

Sensitive Compartmented Information (SCI) – Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of Central Intelligence. [DCID 1/19]

Sensitive Information – Information whose loss, misuse, or unauthorized access to, or modification of, could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or and Act of Congress to be kept secret in the interest of the national defense or foreign policy. Systems that are not national security systems, but contain sensitive information are to be protected in accordance with the requirements of the Computer Security Act of 1987 (P.L. 100-235). [NSTISSI No. 4009, 1996]

Synchronous Communications – Transmission method in which a clock signal is required to align data transmissions. [Pfaffenberger, Brian, PhD, *Que's Computer User's Dictionary*, 1990]

Technical Architecture – A minimal set of rules governing the arrangement, interaction, and interdependence of the parts or elements whose purpose is to ensure that a conformal system satisfies a specified set of requirements. [http://call.army.mil/cal/thesaur/index.htm]

Technical Attack –. An attack that can be perpetrated by circumventing or nullifying hardware or software protection mechanisms, or exploiting hardware or software vulnerabilities, rather than physical destruction or by subverting system personnel or other users. [NSTISSI 4009, 1992; DODD 5160.54]

Telecommunications – 1. Preparation, transmission, communication, or related processing of information (writing, images, sounds, or other data) by electrical, electromagnetic, electro-mechanical, electro-optical, or electronic means. [NSTISSI 4009, 1996] ; 2. Any transmission, emission, or reception of signs, signals, writings, images, sounds, or information of any nature by wire, radio, visual, or other electromagnetic systems. [Joint Pub 1-02, 1994]

Threat – Any circumstance or event with the potential to cause harm to an AIS in the form of destruction, disclosure, modification of data, or denial of service. [JIWG Proposed Common Terminology]

Transmission Security (TRANSEC) – Component of communications security that results from the application of measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis. [NSTISSI 4009, 1996]

Verifiability/Verification – The process of comparing two levels of system specification for proper correspondence (e.g., security policy model with top-level specification, top-level specification with source code, or source code with object code). This process may or may not be automated. [NCSC TG-004]

Virtual – A distributed organization or element which can meet mission requirements without a static spatial frame of reference. [ASD/RA derived]

Virtual Drilling – Participation in a unit training assembly (or mission) without a static spatial frame of reference through the use of collaborative planning tools, telecommuting, and/or other techniques. [ASD/RA derived]

Virtual Network – 1. A network that provides virtual circuits and that is established by using the facilities of a real network [FS -1037C, 1996]; 2. A network that is constructed by using public wires to connect nodes. For example, there are a number of systems that enable one to create networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted. [PC Webopaedia, 1997]

Virtual Private Networks – Enterprise internetworks operated over the Internet. VPN works by using encryption to "tunnel" through switched virtual circuits (SVC) that navigate over a number of intermediary LANs in order to reach remote enterprise locations. A typical VPN scenario is for an enterprise to run through a Tier 1 ISP and purchase SVCs to each remote site. The SVC assures that messages will be routed in such a way that performance and security are optimized. Routers

must be configured to perform the encryption and decryption operations. [*Professional Network Library*, Osborne / McGraw-Hill, Copyright 2000]

Vulnerability Analysis/Assessment – Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. [USAF Manual 33-270; NSTISSI No. 4009, 1999]

Web Server – A computer that delivers (serves up) Web pages. Every Web server has an IP address and possibly a domain name. For example, if you enter the URL, http://www.sandybay.com/index.html, in your browser, this sends a request to the server whose domain name is sandybay.com. The server then fetches the page named index.html and sends it to your browser. Any computer can be turned into a Web server by installing server software and connecting the machine to the Internet. There are many Web server software applications, including public domain software from NCSA and commercial packages from Microsoft, Netscape and others. [PC Webopaedia, 1997]

Wide Area Network (WAN) – Computer network that services a large area. WANs typically span large areas (i.e., states, countries, and continents) and are owned by multiple organizations. [USAF Manual 33-270]