DEPARTMENT OF DEFENSE
OFFICE OF FREEDOM OF INFORMATION
1155 DEFENSE PENTAGON
WASHINGTON, DC 20301-1155

MAY 1 4 2007

Ref: 07-F-0232

Ms. Marcia Hofmann
Staff Attorney
Electronic Frontier Foundation
1875 Connecticut Ave., N.W.
Suite 650
Washington, DC 20009

Dear Ms. Hofmann:

This is the final response to your November 2, 2006, Freedom of Information Act request for all agency records from January 1, 2002, to the present describing the activities of the Army Web Risk Assessment Cell, including, but not limited to: "(1) emails, letters, statements, memoranda, or correspondence providing guidance or criteria to or from the Army Web Risk Assessment Cell on how to conduct Internet surveillance and/or monitoring; (2) records describing how data collected by the Army Web Risk Assessment Cell is retained, secured, used, disclosed to other entities, or combined with information from other sources; (3) any guidance or requirements issued to soldiers on blogging or posting material on the Internet; (4) all requests or orders from DOD officials to soldiers concerning revision or deletion of material from soldiers' blogs or websites; (5) all records concerning and/or discussing the applicability of the Privacy Act of 1974 to the Army Web Risk Assessment Cell's collection of information about bloggers; and (6) all review or audits conducted on the implications of military blogging and the Army's surveillance and/or monitoring thereof." I apologize for the delay of this response, which was caused by the need to consult with other Department of Defense (DoD) components.

The Office of the Under Secretary of Defense, Intelligence (OUSDI) conducted a search and identified the enclosed documents, totaling 39 pages, as responsive to items (1), (2), and (6) of your request. No documents responsive to items (3) through (5) were identified. The documents were additionally reviewed by the Department of the Army and U.S. Strategic Command. Mr. John Smith, an Initial Denial Authority (IDA) for OUSDI determined that portions of the enclosed documents contain information exempt from release pursuant to 5 U.S.C. § 552(b)(6), which pertains to information the release of which would constitute a clearly unwarranted invasion of the personal privacy of third parties and Commander Frank A. Colon, an IDA for the U.S. Strategic Command, has additionally determined that information is exempt from release pursuant to 5 U.S.C.§ 522(b)(2), which pertains to purely internal agency rules and practices and 5 U.S.C. §

552(b)(5), which pertains to certain inter- or intra-agency communications protected by the deliberative process privilege.

If you are not satisfied with this action, you may submit an administrative appeal to James Hogan, Chief, Policy, Appeals and Litigation Branch, Office of Freedom of Information, 1155 Defense Pentagon, Washington, D.C. 20301-1155. Your appeal should be postmarked within 60 calendar days of the date of this letter, should cite to case number 06-F-0232, and should be clearly marked "Freedom of Information Act Appeal." There are no fees associated with this response.

Sincerely,

for Will Kammer
Chief

Enclosures:
As stated

[redacted]

From: JWRAC [jwrac@cert.mil]
Sent: Friday, August 13, 2004 1:11 PM
To: [redacted] JWRAC
Subject: Conference Minutes/Presentations are Posted to SIPR

Attachments: minutes_q4_2004.doc; attendees_q4_2004.doc


minutes_q4_2004.doc (31 KB) attendees_q4_2004.doc (664 KB)...

For those who do not have SIPRNET access, I am providing you with the meeting minutes and attendee list. The presentations slides can be found posted to the JWRAC Conferences link on the DoD CERT SIPRNET web page www.cert.smil.mil.

<<minutes_q4_2004.doc>> <<attendees_q4_2004.doc>> Thanks to everyone for your participation and ongoing efforts!

[redacted] Maj, USAF
Ch, Vulnerability Analysis
[redacted]

JTF-GNO/J32
PO Box 4502
Arlington, VA 22204-4502

JWRAC Conference Minutes
Arlington, VA
3-5 Aug 2004

Attendees:
(attendees_q4_2004.doc)

Executive Summary:
Since the last conference, several improvements have been made to move the web risk assessment mission forward. Improvements in both Coast and White Oak products are providing improved capability and efficiency. Relationships established with OSD offices and STRATCOM appear encouraging as we work to establish policy to deal with the risk posed by publicly available DoD web content. In addition, the move of JWRAC to the newly established JTF-GNO will give its operations a more operational flavor. As the web risk assessment mission continues to evolve, the synergy of these conferences will help to ensure continued success.

The main focus of the conference was how to bridge the different approaches being used to address web risk. It is apparent that some service WRACs focus mainly on compliance and address OPSEC concerns as they arise, while others focus on OPSEC alone. Discussion held with participants from OSD, AF/XO, and STRATCOM are encouraging. Without additional guidance, however, the gap between the WRACs will grow even wider.

The next WRAC conference will be held in November 2004 in Norfolk, VA and is expected to be a two-day conference. The focus will be on determining how the Coast and White Oak tools compare to determine how they might be used in conjunction.

JWRAC Briefing:
-- JWRAC moved under JTF-GNO/J-3
-- Seeking ways to focus efforts, requires access to intelligence community
-- Performed 2 Open Source Assessments
-- Kicked off harvest...eliminated images and changed to Jr Analyst to reduce costs
-- Pursuing 4 goals...standardize processes, secure manpower, improve harvest, establish metrics
-- On-going efforts
  --- Reporting criteria and process
  --- Formulation of policy with OSD
  --- Integrating public affairs at the DoD level
  --- Formulation of doctrine with the Joint Staff

FIWC Briefing:

FIWC-WRA Mission:

Ensure web pages resident on WWW are in compliance with prescribed guidance, and benefits provided through www are balanced with the protection of operations, personnel and privacy.

-- Overview of original tasking, mission, organization and Navy guidance to webmasters
-- Overview of resources, organizations, hardware, software
  --- No funding specifically for WRA mission
  --- Identified need to formally task Navy/FIWC with the WRA mission
-- Overview of training plan/qualifications
-- Overview of Coast development/implementation
-- Recommended standardizing training and reporting
-- Expressed need to capture and publish lessons learned
-- Ongoing challenges:
  --- Need for dual assessments (.mil vs .com views)
  --- NMCI webmasters providing 24x7 support
  --- Fine tuning use of Coast tool
  --- PKI issues preventing access

AFWRAC Briefing:

AFWRAC Mission

Analyze all AF owned, leased, or operated web sites and identify information not approved for public release, reveals personal information on our people or reveals on-going or planned operations.

-- Overview of mission and tasking (68 IOS took mission on 1 Apr 04)
  --- In support of Electronic Systems Security Assessment (ESSA) tasking requests
-- Provided update on their use of JWDTS (22 of 37 reports closed, process is slow)
-- Provided update on use of Coast product
  --- Initially assessing .com accessible web sites only, seeking approval to assess NIPR
-- Partnering w/AFNEWs to take proactive approach to assess web pages prior to posting
-- Seeking to sustain through Unfunded Requirements requests

AWRAC Briefing:

AWRAC Mission

Review the content of Army's publicly accessible Web sites. The AWRAC conducts ongoing operational security and threat assessments of Army Web sites (.mil and all other domains used for communicating official information) to ensure that they are compliant with DOD and Army policies and best practices. (Published in AR-25-1)

-- Overview of organizaton, mission, and findings, lessons learned
-- Provided overview of automated training system (provides reusable tests)
  --- Tapped existing training contract to develop WRAC training modules

MARWRAC Briefing:

-- [redacted] unable to attend (OBE)

--- Sole Marine member responsible for WRA along with additional IA/CND functions

Coast Software Briefing:

-- Overview of Coast Software, Inc. history, customers, focus, products

-- Provided overview of features of settings, reports, drill down ability, links to references

-- WRAC influence

--- Established web registration plug-in and discrepancy management database

--- Expanded ability to set site rules in addition page rules

--- XML compliant to support JWRAC baseline

--- All four Services using Coast

White Oak Briefing:

-- Overview of harvest process and update on harvest currently underway

-- Provided overview of development efforts to improve functionality of JWDTS

--- Based on baseline functional requirements identified last conference

-- Provided update on efforts in developing a training manual – expect by end of Aug 04.

-- Next harvest will start immediately after current harvest complete

STRATCOM Briefing:

-- Overview of STRATCOM organization and IO Roadmap

--- OPSEC recommendations to IO Roadmap include:

----Enhamcing OPSEC support (Joint OPSEC Support Element (JOSE) - Oct 04)

---- Revise OPSEC policy/doctrine (DoD 5205.2 and JCS Pub 3-54 under review)

---- Institute vulnerability assessments **(possible inclusion of WRAC mission)**

---- Provide command emphasis (OPSEC management/oversight support to CCs)

-- Overview of Joint Information Operations Center (JIOC)

-- Overview of STRATCOM role (advocating/adjudicating/providing vision for OPSEC)

OSD(PA) Briefing:

-- Provided overview of recommended web content policies/guidelines for federal web

--- E-Gov Act is driving force with FirstGove.gov taking lead role

--- Recommendations submitted to OMB

-- Overview of 7 policy recommendations

--- Authenticity, branding and timeliness must be ensured

--- Web sites must be written from audience point of view

--- Ensure web sites designed and written to ensure easy access and use

--- Simplify and unify information across the government

--- Agencies must establish priorities and schedule for posting content to web sites

--- Ensure compliance with existing Federal laws, regulations and policies

--- Establish structure/process for establishing web content policy

-- Recommendations submitted to OMB…expect final OMB guidance by Dec 04

-- Provided a definition of Publicly Accessible, definition supported by WRACs

OSD(NII) Briefing:

-- Overview of how move to net-centric DoD will impact how information is processed
-- Overview of Net-Centric Initiatives currently underway
-- Overview of Net-Centric Checklist for future initiatives
-- Highlighted challenges of web services
  --- Dynamic web pages
  --- Database driven content
-- Highlighted goals today's efforts must address
  --- Provide real-time situational awareness (automation)
  --- Ability to evaluate/assess risk in web services environment (overcoming obstacles)
  --- Ability to provide a joint response
  --- Move toward privatization/outsourcing (impact on 24x7 response, mitigation)

Open Discussion:

(discussion_notes_q4_2004)

Action Items:

-- JWRAC: Send regulatory document links for service WRACs to identify overlaps
-- JWRAC: Consolidate WRAC policy inputs and provide to OSD for consideration
-- JWRAC/AFWRAC: Compare capabilities of harvest and Coast tool
-- JWRAC: Develop a robust web site on NIPR/SIPR to advertise efforts/provide info
-- Service WRACs: Provide JWRAC with links to be included on JWRAC web page
-- Consider ways to capture and publish lessons learned

Quarterly WRAC Conference

3-5 August 2004

HQ DISA, Arlington, VA

Name	Organization	Phone Number	E-mail
[redacted]	JTF-GNO	[redacted]	[redacted]
	AF/XOIW		
	68 IOS		
	COAST Software		
	FIWC		
	NETCOM AWRAC		
	JHU/APL		
	JHU/APL		
	CNSG		
	JFHQ-IO		
	OSD-NII/DCIO		
	ISSO		
	ISSO		
	JTF-GNO		
	OSD(PWPO)		
	OUSD(I) DUSD(CI&S)		

[redacted] CTR OSD OUSDI

From: JWRAC [jwrac@cert.mil]
Sent: Friday, November 05, 2004 9:55 AM
To: [redacted]

Subject: Meeting Minutes from 26-27 JWRAC Conference

Follow Up Flag: Follow up
Flag Status: Green

Attachments: minutes_q1_2005.doc; attendees_q1_2005.doc; AFWRAC Enabling Concept - Oct 04.doc


minutes_q1_2005.doc (34 KB)


attendees_q1_2005.doc (21 KB)


AFWRAC Enabling Concept - Oct ...

Classification: UNCLASSIFIED

Caveats: NONE

In addition to the minutes and attendee listing, I am providing you with a the AFWRACs draft ConOps. The AFWRAC JQS training docs and the JWRAC's TTP for performing Open Source Assessments, and OPSEC POC list are expected by the end of the month for your review.

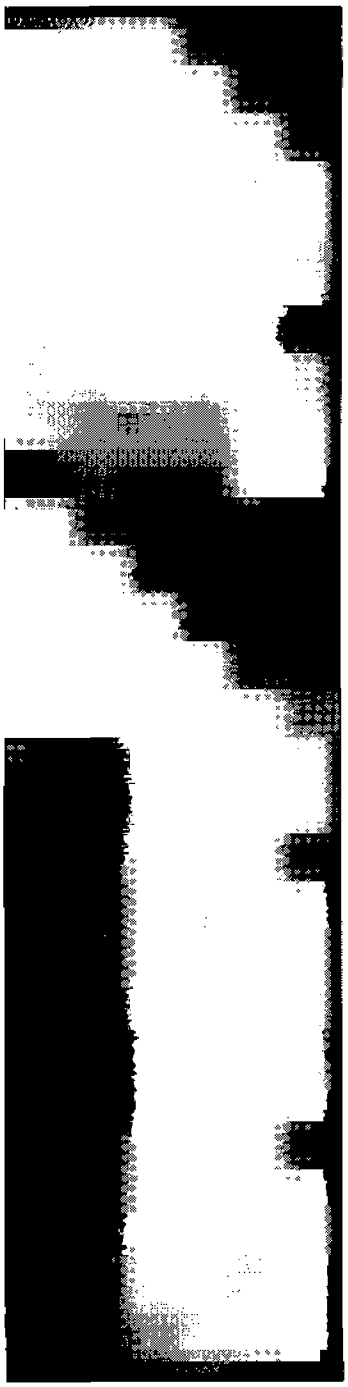
<<minutes_q1_2005.doc>> <<attendees_q1_2005.doc>> <<AFWRAC Enabling Concept - Oct 04.doc>> I want to once again thank everyone for coming together and sharing your efforts to improve web risk assessment! I think you are making a difference and we are making progress! I will have the briefing slides posted soon to SIPRNet at http://www.cert.smil.mil/jwrac/jwrac_conference.htm

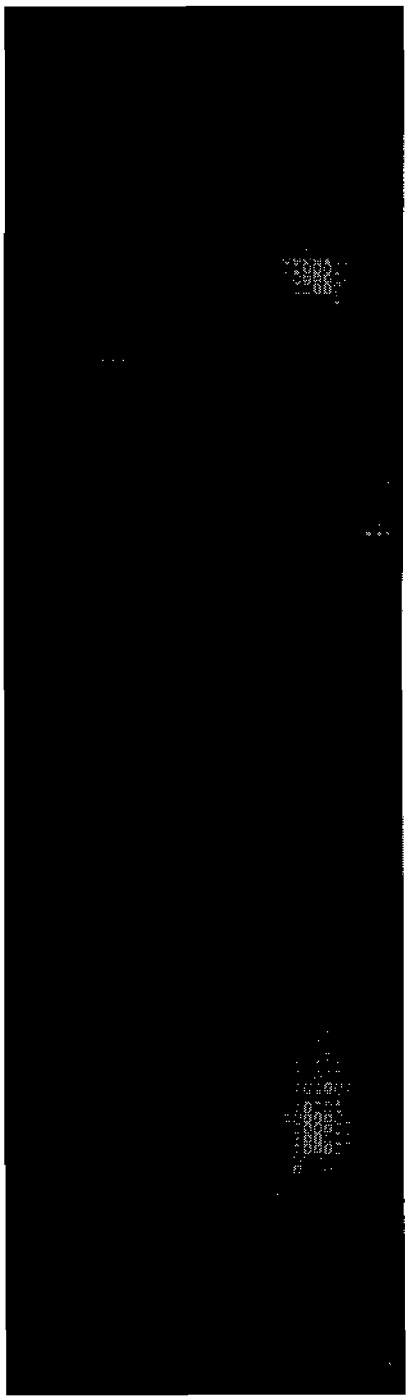
Please contact JWRAC@cert.mil if you have any questions or need additional information.

[redacted] Maj, USAF
Ch, Vulnerability Analysis
[redacted]

JTF-GNO/J32
PO Box 4502
Arlington, VA 22204-4502

Classification: UNCLASSIFIED
Caveats: NONE





JWRAC Conference Minutes
Norfolk, VA
5-6 Oct 2004

Attendees:
(attendees_q1_2005.doc)

Executive Summary:
Progress continues as we work to improve the capabilities of the tools being used to accomplish the web risk assessment mission. The Navy continues to take the lead in developing Coast, the COTS software each of the service WRACs are using to scan and assess web sites. A backend database has now been integrated that allows discrepancies to be tracked and serves a dual purpose as a web site registration system. Web sites can be registered in this system either manually or through a discovery process that occurs during scanning and then uploaded into GILS. The other services are still struggling to get funding to sustain their operations, much less invest in a tools that provide such capability. The AF was able to obtain some funding, but future funding, even for the Navy's web risk assessment operations is uncertain.

The guest speakers provided insight into their efforts to improve web risk assessment in their area of influence. The JWRAC welcomed a 1st IO Command rep who provided insight on how their operations under the Army G-3 are related to the AWRAC's operations which exist under the Army G-6. A rep from the Interagency OPSEC Support Staff, responsible for providing OPSEC training to DoD and other federal agencies informed us of a new course being developed called "Web Risk Assessment." Although the OSD(NII) rep was unable to attend, she provided info to the JWRAC on a draft OMB recommendation for managing information on the web. The recommendation is expected to go final in Dec '05 and may impact web risk assessment operations.
And AF/XOI briefed on their efforts to formally establish an AF Web Risk Assessment Program.

The web risk assessment mission continues to gain momentum as we continue working to establish a reporting process, standardize where we can, and establish funding to sustain operations. The next WRAC conference will be held in March 2005 in Austin, TX and is expected to be a two-day conference. The focus will be on reporting, web pages, tool integration, and impact of STRATCOM re-structuring of its IO operations.

JWRAC Briefing:
-- Covered Action Items from last conference
  --- Unable to compare harvest with Service WRAC Coast tool.
  --- Web Site development is underway
-- Harvest complete. Requirements for quarterly reports need to be nailed down
-- Provided overview of recommended quarterly report requirements
  --- Harvest Stats (avg time to remediate web discrepancies – over 34 days)
  --- Summary of all WRAC findings

--- Recommended using 'balanced scorecard' approach to reporting
--- Goal is to establish process and begin reporting in Jan '05
-- JWDTS Training Guides developed and out to WRACs for constructive feedback
-- Provided overview of workshop agenda
--- Standardize content of Initial Notification Messages
--- Refine web page requirements
--- Determine initial reporting capability
-- Provided update on JWRAC activities over past quarter
--- Attendance at OPSEC Community of Knowledge and Practice
--- Efforts to improve manpower
--- Ongoing discussions with Joint Staff, OSD, STRATCOM, and others
--- Completion of OSA for PACOM, Request for OSA received from TRANSCOM

FIWC Briefing:

FIWC-WRA Mission:

Ensure web pages resident on WWW are in compliance with prescribed guidance, and benefits provided through www are balanced with the protection of operations, personnel and privacy.

-- Provided overview of mission, current environment, organization, and tools
-- Introduced group to latest development of their COTS web scanning and tracking tool
--- Development of a back-end Discrepancy Management System database with reports
--- A web site registration/validation interface that can be used to upload data into GILS
-- Provided update on assessment findings over the past quarter
-- Identified ongoing challenges
--- Funding, standardization, and training
--- Ongoing refinement of Coast product
-- Request to pursue .com connection approved...will allow .com view of navy sites

AFWRAC Briefing:

AFWRAC Mission

Analyze all AF owned, leased, or operated web sites and identify information not approved for public release, reveals personal information on our people or reveals on-going or planned operations.

-- Provided overview of process – base-level assessments, MAJCOM assigned bases
-- Provided update on JWDTS remediation efforts
--- 5331 discrepancies identified by harvest
--- 51% remediated
--- FOUO and STINFO data made up majority of harvest findings
-- Provided update on use of Coast product
--- Completed 28 base-level scans
--- OPSEC info and personal data made up majority of COAST findings
-- Developed AFWRAC ConOps and Job Qualification Standards
-- Consolidating AF websites to Montgomery AL – will enhance assessment efforts
-- Secured $45K for FY05 operations-working to establish baseline funding requirement

AWRAC Briefing:

AWRAC Mission

Review the content of Army's publicly accessible Web sites. The AWRAC conducts ongoing operational security and threat assessments of Army Web sites (.mil and all other domains used for communicating official information) to ensure that they are compliant with DOD and Army policies and best practices. (Published in AR-25-1)

-- Unable to attend conference, but provided update on recent harvest efforts
--- 2982 discrepancies identified by harvest
---- 12% false positives
---- 73% remediated
---- Personnel and Operation information make up majority of discrepancies - 42.2%
--- Used Coast to review 92 sites

MARWRAC Briefing:

-- MSgt Combs unable to attend - transferring mission to contractor
-- Unable to contact replacement prior to conference—effort ongoing
-- JWRAC will continue to encourage participation by MARWRAC

Coast Software Briefing:

-- Provided update on Coast Software developments since last conference
--- Highlighted integration of discrepancy tracking database into product
--- Introduced the web registration system capable of an automated discovery process
-- Provided a demonstration of the Coast Software
--- Demonstrated the software's ability to provide cradle to grave web site management
--- Provided an overview of the reporting and demonstrated drill down capability

White Oak Briefing:

-- Provided harvest results – took 3 ½ months to complete
-- Improvement efforts identified – moving to ongoing incremental harvest process
-- Provided overview of development efforts
--- JWDTS now supports XML to allow import and export of JWDTS data
--- Team Chief/Analyst Training guides developed – WRAC Chief guide on the way
--- Poised to continue training efforts – Administration and Advanced Guides possible

OSD(NII) Briefing:

-- Unable to attend conference, but provided JWRAC with update on OMB efforts that may impact operations
-- EGovt Act of 2002 requires OMB to provide recommendations on web management
--- Electronic Records Policy
--- Web Standards
--- Categorization of Information
-- Final OMB recommendation out for comment – expect final in Dec '04
--- Registration requirements more stringent
--- All DoD-sites in .mil domain

--- Dual language requirement for publicly accessible web sites (Korean/English?)
--- HTTPS sites not exempt
--- Only non-public web site is logon/password protected

AF/XOI Briefing:

-- Taking multi-faceted approach to address web risk assessment in the Air Force
--- AF/XO memo in draft that formally establishes AFWRAC program
--- Memo assigns Air Combat Command as lead
--- AFWRAC developing ConOps
--- AFI being developed to establish program procedures
--- Recommending a formal reporting process for reporting AFWRAC findings
--- AF/PA, webmasters, and AFWRAC members training requirements being identified
-- Goal is to establish formal program by Mar '05

1st IO Command Briefing:

-- Overview of 1st IO Command's Vulnerability Assessment Division's organization and mission
-- Provided insight on the focus of their operations, their concerns, efforts under way
-- Shared lessons learned and challenges that need to be overcome
-- Emphasized the need to bring Web Masters, Public Affairs and OPSEC Officers together to affect change.

Action Items:

-- Distribute AFWRAC ConOps and Job Qualification Standards to all WRACs
-- Provide each Service WRAC with Qualified Domain Name List from harvest – 12 Nov
-- Distribute Open Source Assessment TTP to Service WRACs – 12 Nov
-- Provide training guides – Service WRAC feedback requested - 30 Nov
-- Prepare JTF-GNO announcement to inform DoD Community of WRACs – 30 Nov
-- JWRAC/AFWRAC: Compare capabilities of harvest and Coast tool (ongoing)
-- JWRAC: Develop a robust web site on NIPR/SIPR to advertise efforts (ongoing)
-- Contact Joint OPSEC Support Element to discuss participation at next conference
-- Contact DINFOS to introduce risks web content poses when training in Public Affairs
-- Develop OPSEC POC Listing – 30 Nov
-- Distribute Draft OMB doc to service WRACs for comment – comments due - 5 Nov
-- Prepare reporting requirements to begin reporting in Jan 05

68th INFORMATION OPERATIONS SQUADRON

AIR FORCE WEB RISK ASSESSMENT

ENABLING CONCEPT

October 2004

Prepared by: [redacted]
Operations Officer
68th Information Operations Squadron

Reviewed by: [redacted]
Commander
68th Information Operations Squadron

Approved by: [redacted]
Commander
67th Information Operations Wing

OPR: 68 IOS/DO
Brooks City-Base, TX

FOR OFFICIAL USE ONLY

[redacted] CTR OSD OUSDI

From: JWRAC [jwrac@cert.mil]
Sent: Tuesday, March 22, 2005 12:10 PM
To: [redacted]
Cc:
Subject: JWRAC Conference Minutes

Follow Up Flag: Follow up
Flag Status: Green

Attachments: JWRAC Conference Minutes.doc; Scan0001.tif; Scan0002.tif; Scan0003.tif; Scan0004.tif; JTF-GNO Evaluation of JWRAC Mission ; web policy draft(6Jan05).doc


JWRAC Conference Minutes.doc (...


Scan0001.tif (458 KB)


Scan0002.tif (454 KB)


Scan0003.tif (454 KB)


Scan0004.tif (471 KB)


JTF-GNO Evaluation of JWRAC Mi...


web policy draft(6Jan05).doc (..

Classification: Unclassified
Caveats: None

ALCON,

Attached are the finalized conference meeting minutes for your review. Also attached are copies of the IOTA and CKAP pamphlets distributed at the conference as well as the original e-mail forwarded in February requesting inputs for the JWRAC program review. For those who've replied with your comments, thus far, thank you. I'm still gathering inputs, if anyone else has anything to add. Lastly, is a copy of the draft web policy to be discussed 29 March. Thus, please RSVP with [redacted] NLT 25 March.

<<JWRAC Conference Minutes.doc>>

<<Scan0001.tif>> <<Scan0002.tif>> <<Scan0003.tif>> <<Scan0004.tif>>

<<JTF-GNO Evaluation of JWRAC Mission >> <<web policy draft(6Jan05).doc>>

vr,

[redacted] 1st Lt, USAF
Operations Officer, Joint Web Risk Assessment Cell Joint Task Force-Global Network Operations
[redacted]

Classification: Unclassified
Caveats: None

JOINT TASK FORCE-GLOBAL NETWORK OPERATIONS
P. O. Box 4502
ARLINGTON, VIRGINIA 22204-2199

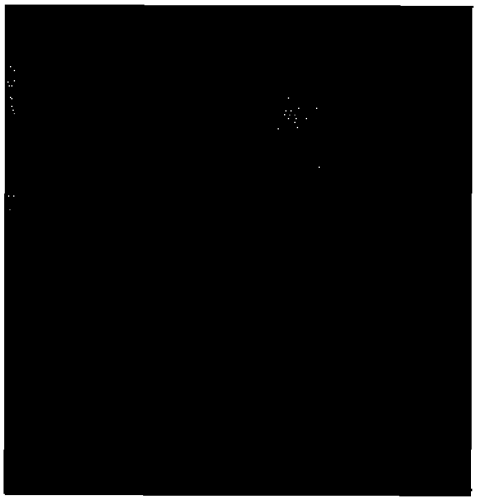
IN REPLY
REFER TO:

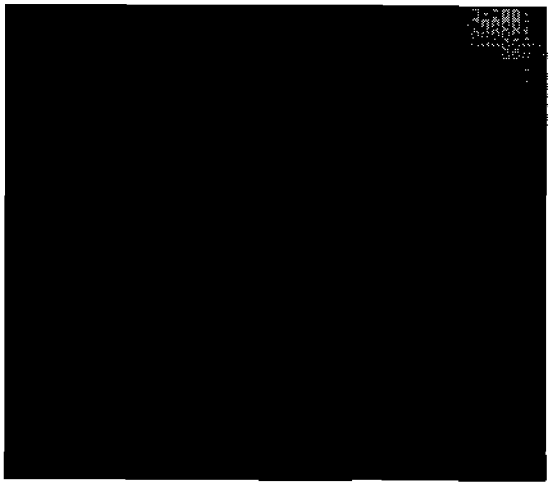
22 March 2005

JTF-GNO/J32

JWRAC Conference Minutes, Austin, TX - 8-9 March 2005

Attendees:





Executive Summary:

Despite the limitations in available resources used to sustain current operations, JWRAC and each of the service web risk assessment cells are continuing their efforts to improving OPSEC security while obtaining advocate support within the DoD community. The JWRAC spoke of its own internal program review, the briefing scheduled for the J-3, JTF-GNO and the courses of action available to determine a logical outcome. Inputs for recommendations, suggestions and such were solicited to help justify the relevancy of JWRAC's existence. A representative from OSD spoke about the revision of the Website Administration and Guidance policy and the impact it will have on the operations for all WRAC activities. Additionally, an invite was extended to anyone in the D.C. area on 29 March to attend a briefing hosted by OSD in reference to web policy.

The JWRAC welcomed some invited guests who were attending the conference for the first time. The Chief of OPSEC at the JIOC provided a brief overview of the operations within the Joint Information Operations Center and their visionary plan to utilizing JWRAC within their new programs. Representatives from the Information Operations Technology Alliance/Community Knowledge and Practice organization provided an insightful briefing on their programs. They

explained how they support DoD in its continuous exploration of new IO concepts, challenges, and possible technology solutions in the government, industry and academia arena.

The next conference will be arranged for four months hence (exact date and location TBD). The focus will be establishing and confirming the roles and relationships amongst the service WRACs, JWRAC and the DoD community.

JWRAC Briefing:
-- Covered action items from the last conference
-- Due to JTF-GNO's web policy a robust NIPR website has not been available. However, upon the merger of the internal networks within JTF-GNO, JWRAC will continue its coordination in establishing a website advertising the mission of JWRAC and the Service affiliates.
-- Open Source Assessments TTPs and the JWDTS manuals have been distributed to the Service WRACs for review. Feedback referencing the JWDTS manuals were received and forwarded to White Oak.
-- Inputs for reporting requirements were discussed at the last conference, but a consensus has yet to be reached. However, due to a reporting channel still not created, this action item was put on hold until further notice.
-- Each service WRAC was provided with a copy of the AFWRAC ConOps and the Job Qualification Standards for review.
-- Unable to contact DINFOS in reference to PAO training. Will coordinate with [redacted] from OSD/USD(I) and [redacted]
-- Forwarded draft OMB policy to each of the service WRACs for review. Inputs were due by 5 Nov 04.
-- Provided each Service WRAC with Qualified Domain Name listing from harvest

FIWC Briefing:
-- Announced that 3600 USN websites have been reviewed at the direction of SECNAV since the last annual review.
-- Reservists were no longer employed in the Navy WRAC due to the problems in proving this a mission worthy with sustainable career development opportunities.
-- Considering reinvesting the WRAC mission within the USN Blue Team to enable breadth of skills and personnel interchangeability.
-- Discussed whether operators who produce information, or the systems owner where the information resides, are the responsible party for OPSEC violations
-- Training for WRAC personnel, PAO, and webmasters were discussed
-- The USN would like to see more advertisement regarding WRAC mission at conferences, training events, etc.
-- 15 Mar 05 the USN will receive a briefing from WATCHFIRE, a competitor of COAST

AFWRAC Briefing:
-- Since the last conference, reports have been completed on ACC, PACAF, and USAFE
-- Currently working on a tasker from AF Space Command
-- PA received a waiver for personal information printed in the base paper. However, OPSEC violations are still reported and handled accordingly.
-- Presented slides showcasing type and number of discrepancies located on each AF base's websites

AWRAC Briefing:
-- Recently purchased Coast Central Compliance software. Team will receive training at the conclusion of the conference
-- Uses both JWDTS and COAST to identify discrepancies within the .mil domain, unlike the Navy who scans from outside the .mil domain.

-- Provided an example of web based training for personnel and agreed to provide a copy to JWRAC if DISA could agree to support it.
-- Looks at NIPRNET and .com sites and uses COAST software to verify discrepancies and load them into JWDTS

AF/XOIW Briefing:
-- USAF has designated WRAC as a capability within a COMSEC/OPSEC focused mission
-- The WRAC is not focused on compliance review for that is the base's responsibility. The WRAC only sample bases, as resources will allow.
-- The WRAC mission is being consolidated within the COMSEC monitoring program. AFI 33-129 will formalize this change and is being staffed this month.
-- A copy of the AFI policy, upon finalization, will be disseminated amongst the Service WRACs for information purposes.
-- Discrepancy information is sent to base POC and PAO for remediation
-- Discrepancies are categorized as either critical or routine
-- Will provide copies of ConOps and Telecommunications and Assessment Program (TMAP), and other policies for JWRAC and the Service WRACS.
-- Discussed whether FOUO could be sent over the NIPRNET

JIOC Briefing:
-- Consists of 300 personnel (military, civilian, and contractor), but no reservists
-- Primarily focuses on program development, surveys, and plans and training
-- Currently constructing the Joint Deployable Operations Cell (JDOC) with the aim of having it effective by the end of this fiscal year.
-- JDOC will conduct assessments for commanders of their IO footprint in theatre. This will be performed using the JMDVA concept, which integrates the capabilities of multiple, separately owned teams into one assessment team.
-- Forecasting 6 reports per year with a 120-day planning cycle. Each Service component would coordinate with respective Service WRAC to receive a general digital presence of their existence on the web and who's linked to it. Execution phase would be 2-4 weeks.
-- JIOC agreed to provide JMDVA ConOps for all members to view.

COAST Briefing:
-- Provided background information and examples of current clientele
-- Introduced the Coast Central Compliance software
-- Identified new US representative as [redacted]

MWRAC Briefing:
-- Provided update to personnel change and the possible incorporation of this mission in the USMC Blue Team
-- WRAC program is in its infant stage. COAST software was purchased but no other resources have been allocated to support this mission
-- 12 reservists based in CA have previously supported this mission but this manning needs to be re-evaluated.
-- Estimated that USMC has 305 publicly accessible websites, but there is little confidence in the accuracy of this amount

OSD Briefing:
-- Provided first briefing on the emerging information exchange policies/developments with other Government departments and the possible use of WRAC services to strengthen trust relationships
-- Second briefing was the development and implications of new web policies
-- Distributed copies of the draft Web policy for feedback

-- New policy will confirm Director of DISA's remit to establish and run the JWRAC, although it doesn't mandate the use of military personnel.
-- It was suggested that JWRAC could potentially perform admin/coord rather than OPSEC missions using reservists
-- Referenced http://www.firstgov.gov/webcontent/index.shtml as a repository for web policies
-- OSD would like to produce a Web Masters Handbook as a reference for web posting and would like to include a WRAC section.

IOTA/CKAP Briefing:
-- Distributed hand-outs illustrating their program
-- Explained that PHOENIX CHALLENGE helped DoD explore new IO concepts, ideas, and technology solutions
-- Representatives from industry, academia and government select which products best supports their overall IO process
-- Products are NIAP approved, but require endorsement by the appropriate DAA authority before they can be used on NIPR/SIPRNET.

ACTION ITEMS:

-- JIOC will forward JMDVA ConOps to JWRAC
-- JWRAC will distribute AFWRAC policy once received from the USAF
-- JWRAC will reissue the standardized previously circulated format of reporting criteria
-- JWRAC will forward OSD policy to service WRACs
-- JWRAC will forward its training roster to MWRAC
-- JWRAC will create a service WRAC matrix describing responsibilities, training, policy, etc
-- JWRAC will forward OSD web policy handbook when published to Service WRACs
All members identify key conferences and briefs where the WRAC mission could be vocalized
-- JWRAC to liaise with DISA regarding the use, or referencing of the Army Web Assessment training tool within the DISA Web Policy CD and the possible inclusion of the OSD Web Masters Handbook, when produced.
-- All meeting members to provide comments for the JWRAC internal program review.
-- USAF to confirm which organization(s) has CIO responsibility for ANG units
-- JWRAC to liaise with OSD regarding possible NIPRNet hosting space for JWRAC website if JTF-GNO are further delayed.
-- OSD to confirm policy for the use of FOUO data over the NIPRNet/Internet.

Attachments:

1. JWRAC Internal Program Review information request.
2. OSD Draft web policy and memo.
3. IOTA and CKAP pamphlets.

CKAP Mission

Promote quick solutions and capabilities from subject matter experts.

Determine best technologies available to solve current IO challenges.

Points of Contact

[redacted]
IOTA Program Management Office
Air Force Information Warfare Center
[redacted]

[redacted]
CKAP Facilitator, Contractor
[redacted]

[redacted]
CKAP Facilitator, Contractor
[redacted]

[redacted]
CKAP Facilitator, Contractor
[redacted]

CKAP

Communities of Knowledge and Practice

Information Operations
IOTA
Technology Alliance

The CKAP initiative is one of the three critical components of the IOTA program. Those components are:

1. **Phoenix Challenge**
2. **IO Technology Repository (IOTR)**
3. **Communities of Knowledge and Practice (CKAP)**

February 2005 Version 2.0

Information Operations

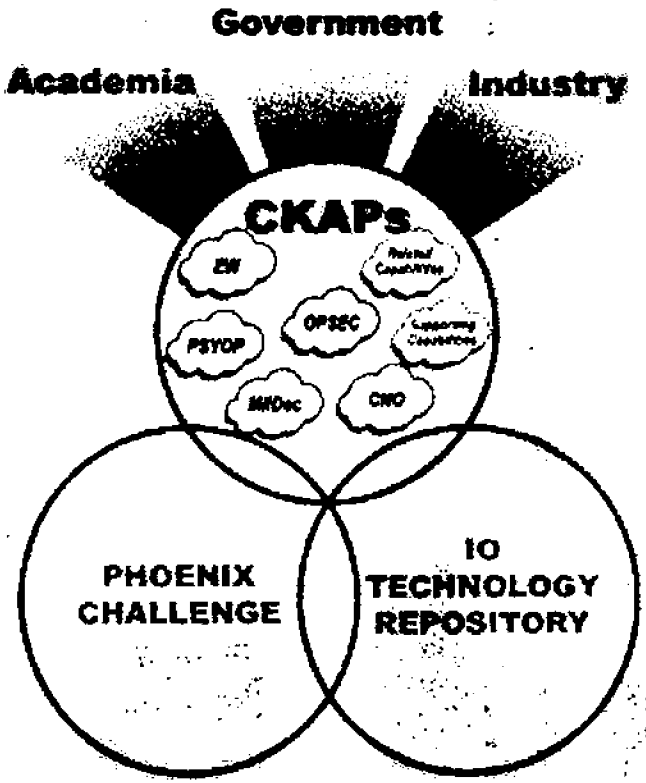
IOTA

Technology Alliance

CKAP Vision

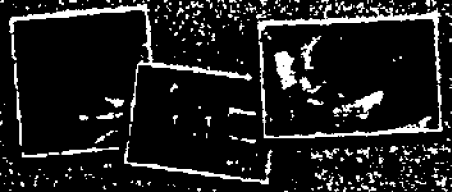
Communities of Knowledge and Practice (CKAPs) will facilitate information sharing between IO disciplines, sub-communities, and interest groups. CKAPs are key to reinforcing expertise and advancing IO knowledge. The role of a knowledge community is to provide a network to more effectively address similar issues and problems. These groups transcend roles and disciplines, and bring together different perspectives. Subject matter experts within the community will meet physically and virtually over time to share insights into IO problem sets. Drawing on the expertise that each member brings to the group, CKAPs will provide a rare environment, supported by facilitation and administrative staff, for focusing creative problem-solving capabilities on the most critical IO issues.

The groups will then have the opportunity to explore, expand and present unique solutions that can be implemented at every level of the IO domain, evolving as community needs and interests change. As part of the complete IOTA effort, the solutions that emerge from CKAP expertise will be looked to by leadership and the community at large to promote rapid implementation in real-world domains.



Phoenix Challenge

Started in 1998, Phoenix Challenge is a professional IO symposium held each year designed to cultivate relationships, information sharing and technology exchanges. Attendees are from the military services, intelligence agencies, other government agencies, industry and academia.



IOTR

The Information Operations Technology Repository (IOTR) will be an online, web-enabled repository and collaborative environment supporting the sharing of information and IO capabilities. IOTR will provide coverage of emerging and existing IO-relevant technologies and concepts to both commercial and Federal IO acquisition and development efforts.

IOTA Charter

Create a technology alliance for DoD and non-DoD government IO professionals. Assist DoD, Industry, and Academia to identify, acquire, and disseminate information on mature and emerging technologies and tools to drive innovation for IO.

IOTA Points of Contact

Air Force Information Warfare Center

[redacted]
IOTA and Phoenix Challenge PM
[redacted]

[redacted]
Chief, Technology Integration
[redacted]

[redacted]
IOTA Operational
and Technical Management
[redacted]

Information Operations
IOTA
Technology Alliance

Three Components of IOTA

1. Phoenix Challenge
2. IO Technology Repository (IOTR)
3. Communities of Knowledge and Practice (CKAP)

February 2005 Version 5.0

1

A professional IO forum creating opportunities to discuss modernization and transformation programs, requirements, challenges and solutions.

Brings together government, industry and academia to share challenges, systems, technologies, and capabilities for IO solutions.

IO Warriors and Technology Experts meet to share the common picture !

- 11th Conference Underway
- Future Conferences Will:
  - Continue allied presence
  - Relevant thematic tracks
  - Enriched by informal meetings

2

Create a knowledge based technology repository for DoD and non-DoD government IO stakeholders.

Leverage DoD, Industry, and Academia developers, to identify, acquire, and disseminate information on mature and emerging technologies and tools that drive IO innovation.

One-Stop Research & Info Shop to Expedite IO Solutions!

- Integrated Operational & System Architecture
  - Version 1.1 Spring 2005
- IOTR System Online
  - Fall 2005

• Questions and Solutions Based	• Virtual Conferencing
Search and Intelligent Retrieval	• Discussion Threads
• Knowledge Discovery	• News Services, Bulletin Boards
• Demonstrations	• Chat, Whiteboard
• Work Flow Management	• List Services

Government • DoD FFRDC • Industry/Academia/Labs

3

IO stakeholders meet physically and on-line to share information on established, maturing, and emerging technologies.

Promote quick reaction solutions and capabilities from subject matter experts. Determine best technologies available to solve current IO challenges.

Informal Groups Meeting to Solve Specific IO Problems!

- Initial CKAP Groups Identified
  - Technology solutions for OPSEC
  - Military Deception
- Information Sharing Successful
  - Cohesive community formed
  - OPSEC Group fully engaged
- Soliciting Topics
  - Priority IO Challenges

[redacted] CTR OSD OUSDI

From: JWRAC [jwrac@cert.mil]
Sent: Friday, February 25, 2005 4:47 PM
To: [redacted]
Cc:
Subject: JTF-GNO Evaluation of JWRAC Mission

Classification: Unclassified
Caveats: None

ALCON,

1. The J3, Director of Operations, in the Joint Task Force-Global Network Operations (JTF-GNO) has directed a program review of the JWRAC's existence and current state of posture. As part of this review, I am inquiring for all to share your thoughts, experiences, recommendations or anything that you would like to provide from your interaction with the JWRAC during the last four years. Specifically, I have been tasked to provide a briefing on the following:

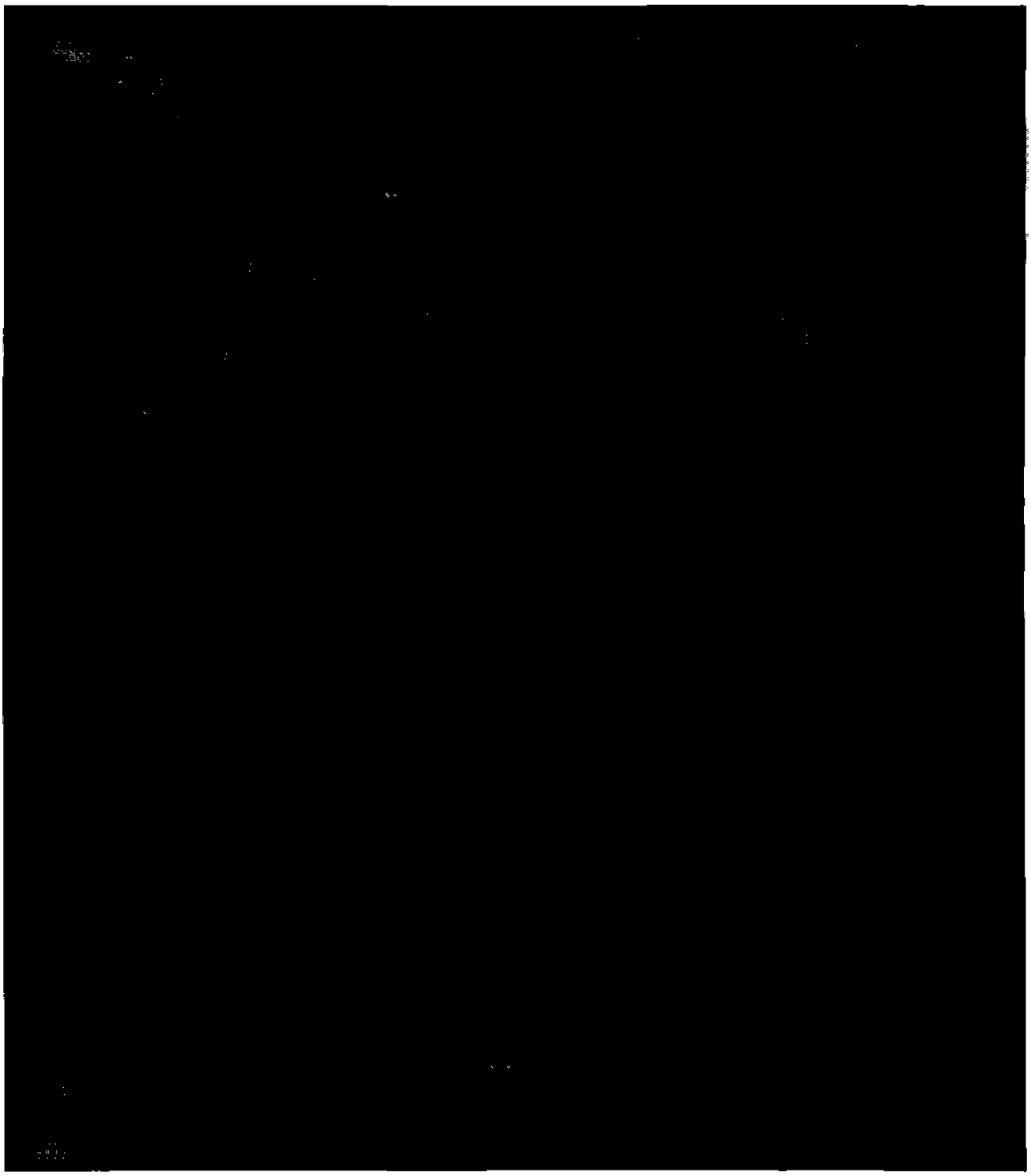
- Background information
- Significant accomplishments
- Tasking priorities/availability
- Funding for personnel and equipment
- Policies (to include policy conflicts and implementation issues)
- Command and control and/or authority of JWRAC tasks/processes
- Command and control of JWRAC resources
- Future mission viability/usefulness
- Relationship with service WRACs and their mission

2. The timeframe allotted for this review is quite short; thus, I would appreciate your responses NLT 18 Mar 05. I will also be attending the JWRAC conference at Camp Mabry, Austin, TX from 8-9 Mar and would be happy to discuss this issue with any attendees during that period.

3. Lastly, I ask that you all include [redacted] in your correspondence at [redacted]@jtfgno.mil as he is [redacted] replacement during her deployment.

v/r,
[redacted] 1st Lt, USAF
Operations Officer, Joint Web Risk Assessment Cell Joint Task Force-Global Network Operations
[redacted]

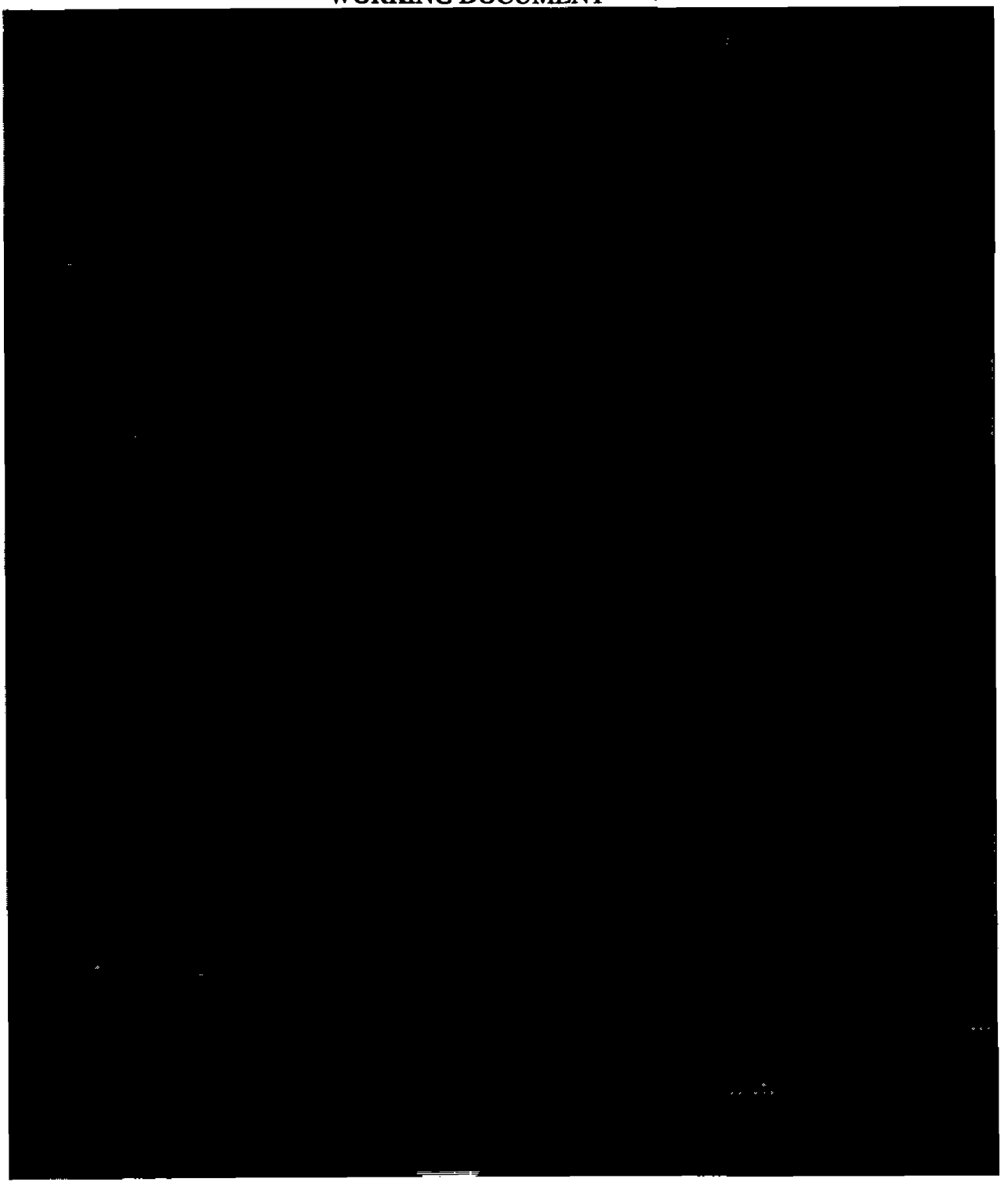
Classification: Unclassified
Caveats: None



DRAFT
WORKING DOCUMENT

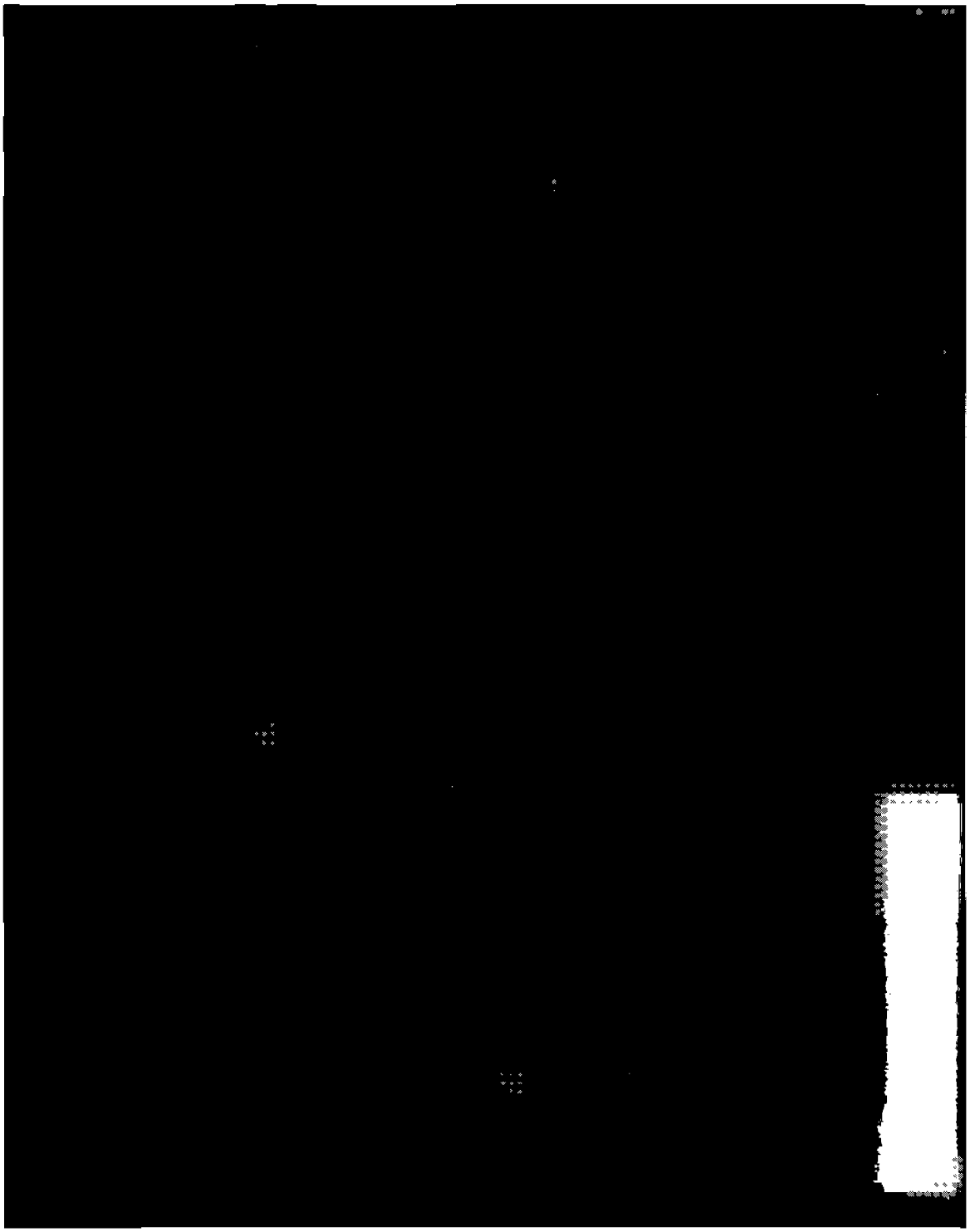
[redacted] Last Updated: 12/7/2006

[redacted]



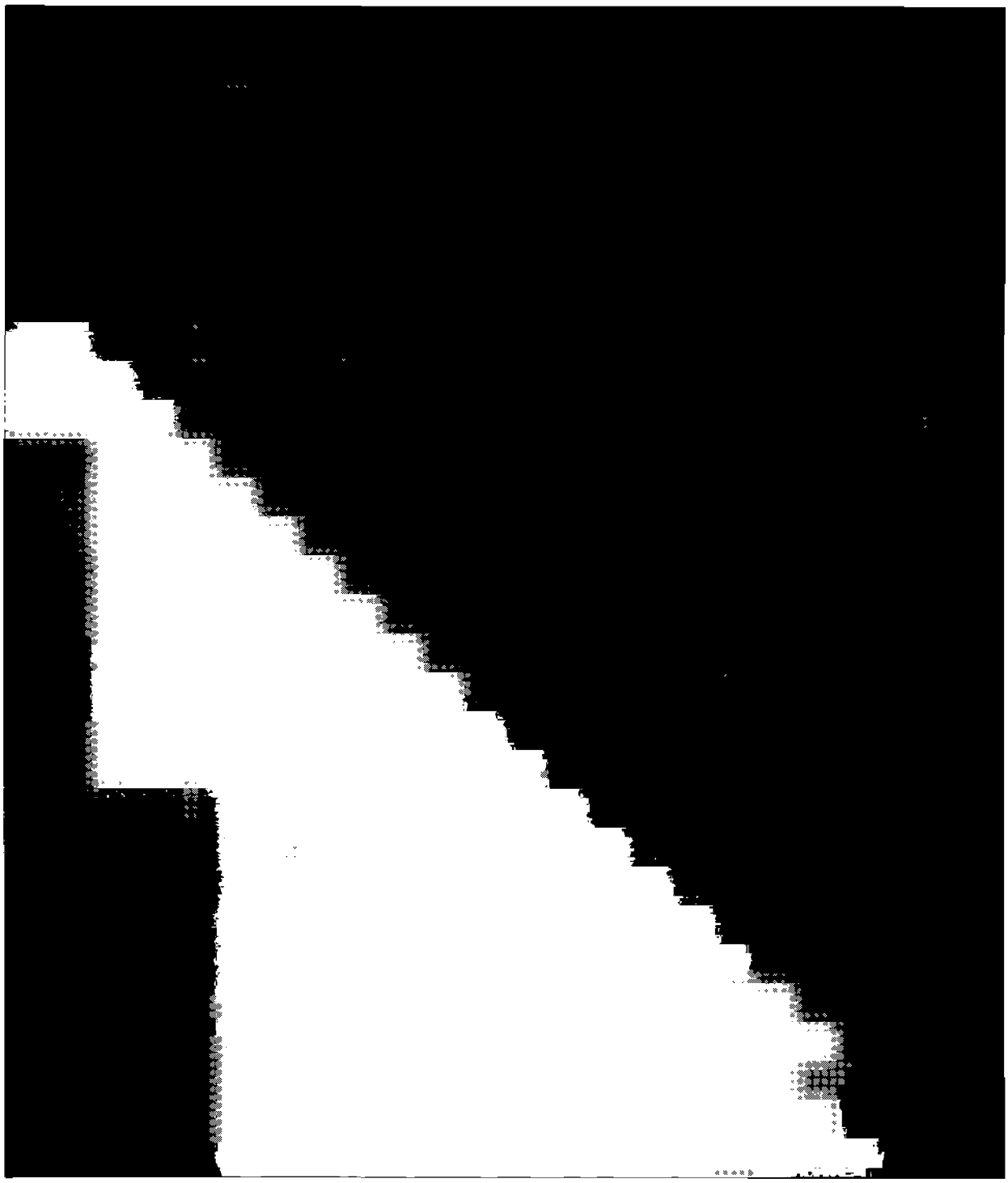
DRAFT
WORKING DOCUMENT

[redacted] Last Updated: 12/7/2006



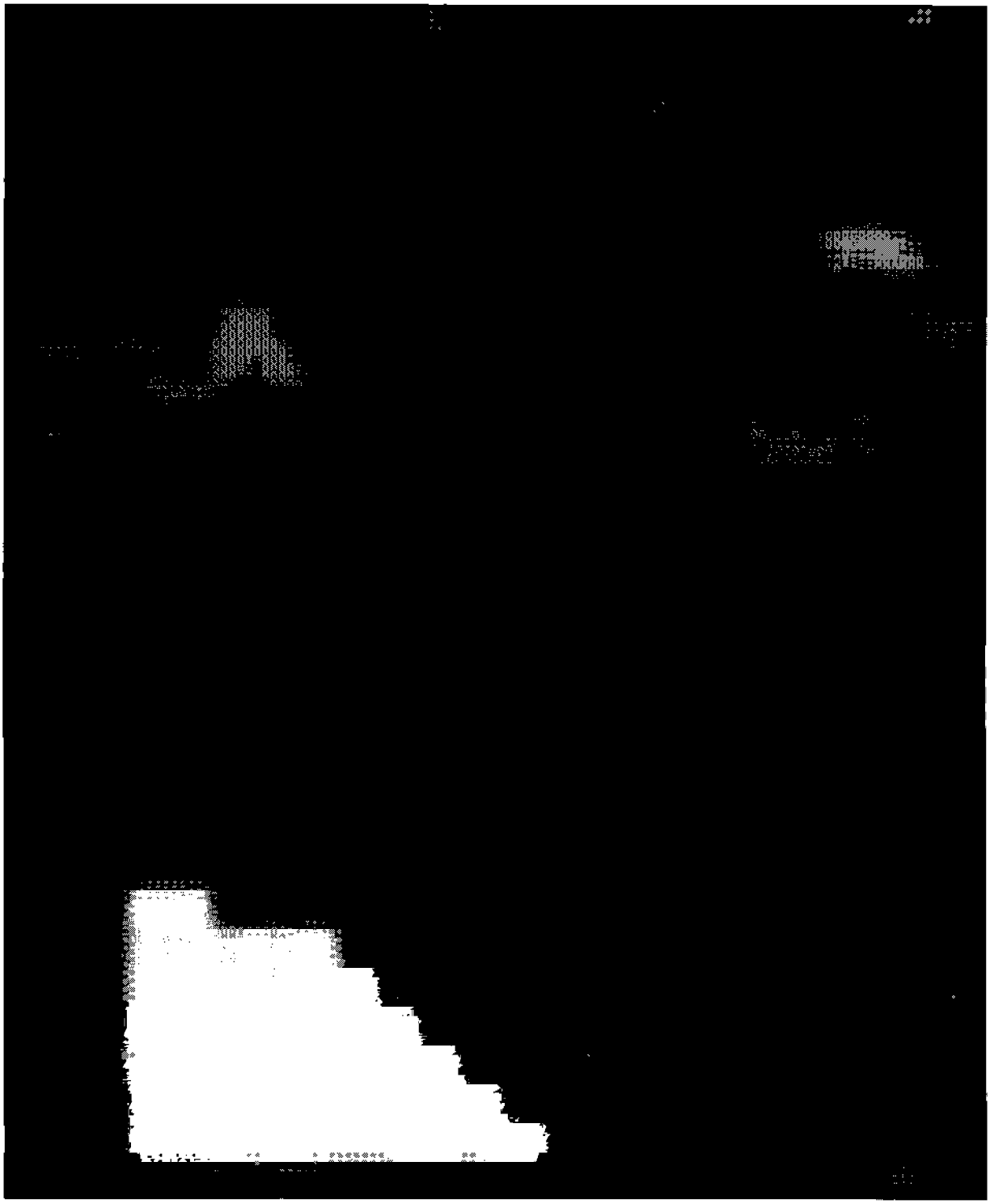
DRAFT
WORKING DOCUMENT

[redacted] Last Updated: 12/7/2006



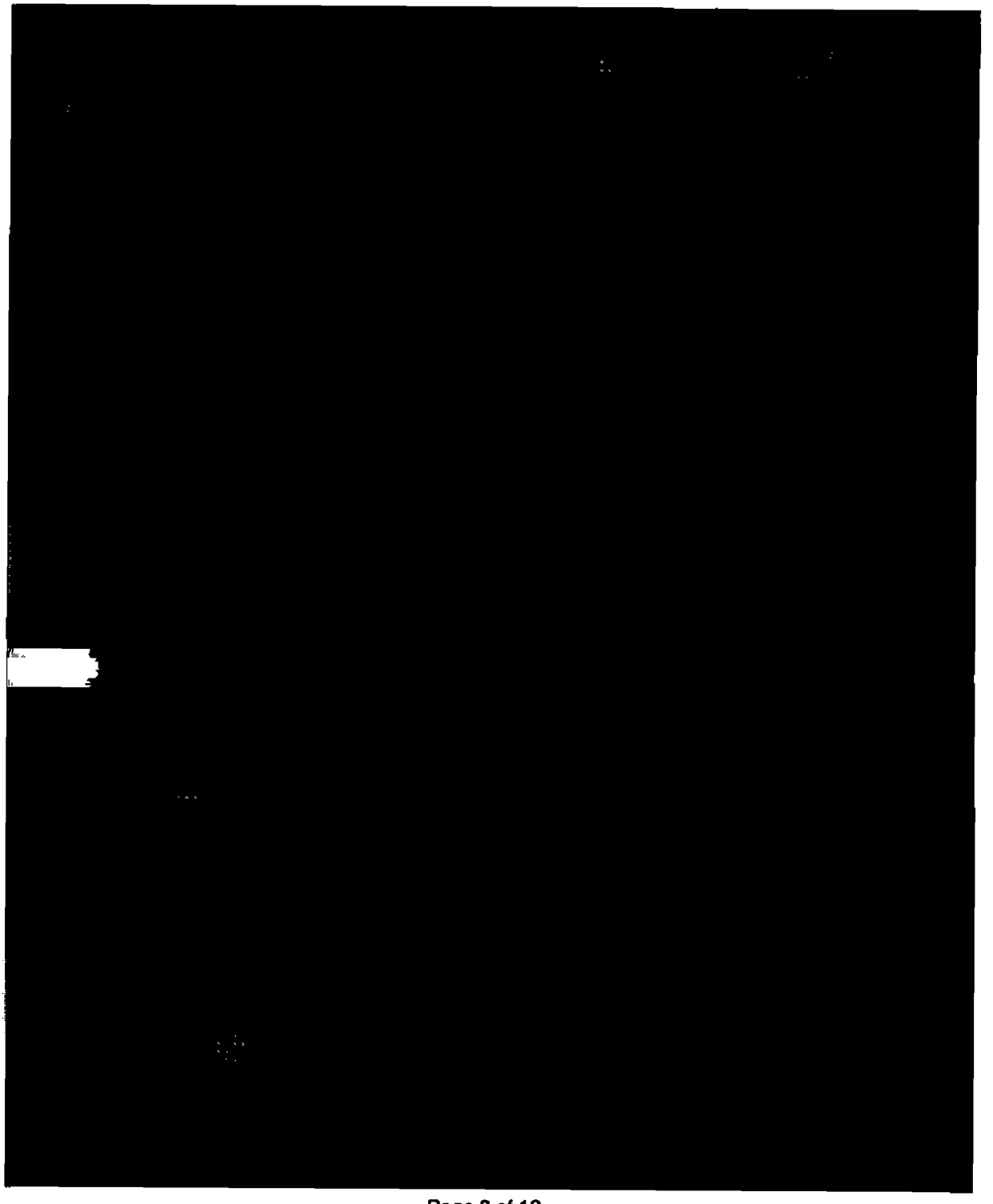
DRAFT
WORKING DOCUMENT

[redacted] Last Updated: 12/7/2006



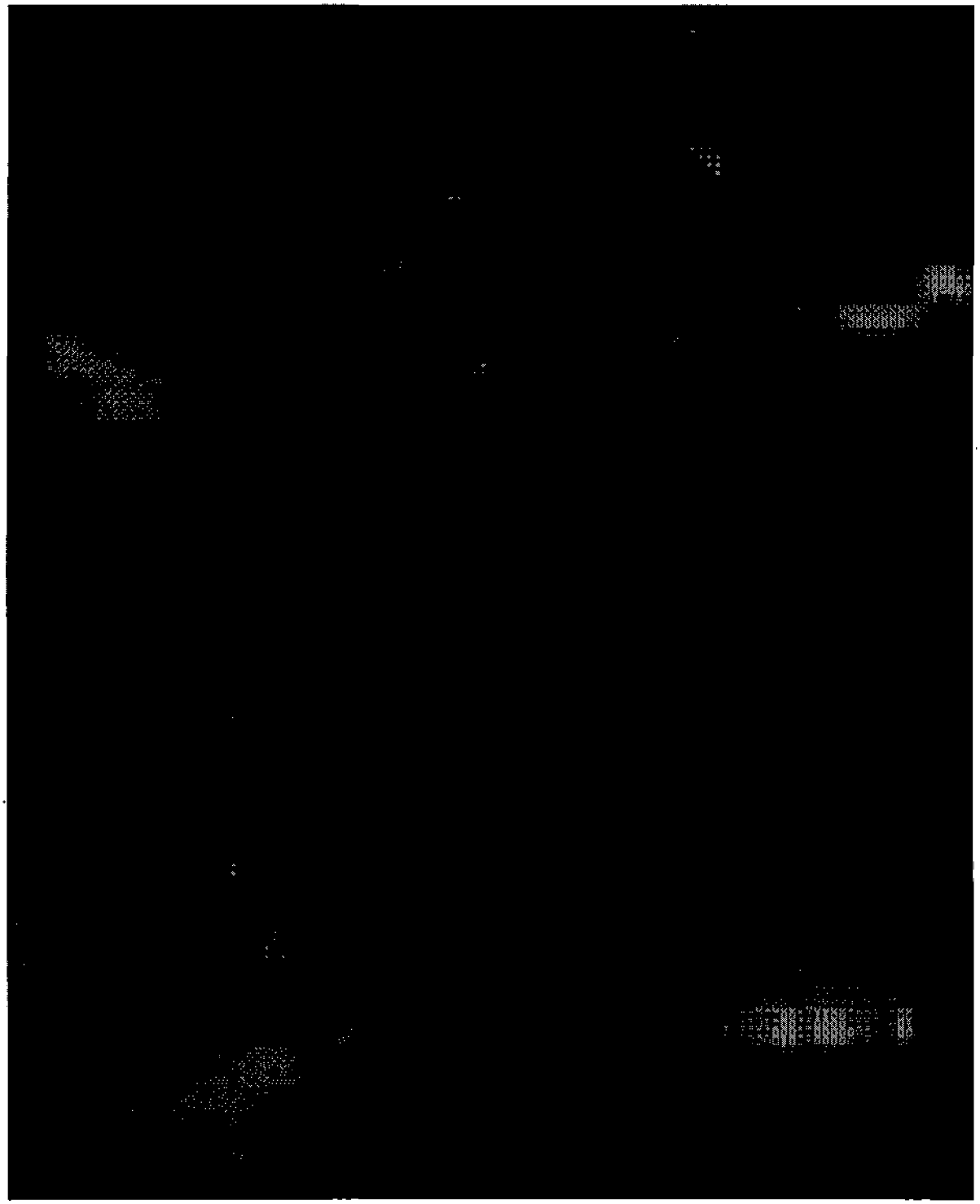
DRAFT
WORKING DOCUMENT

[redacted] Last Updated: 12/7/2006

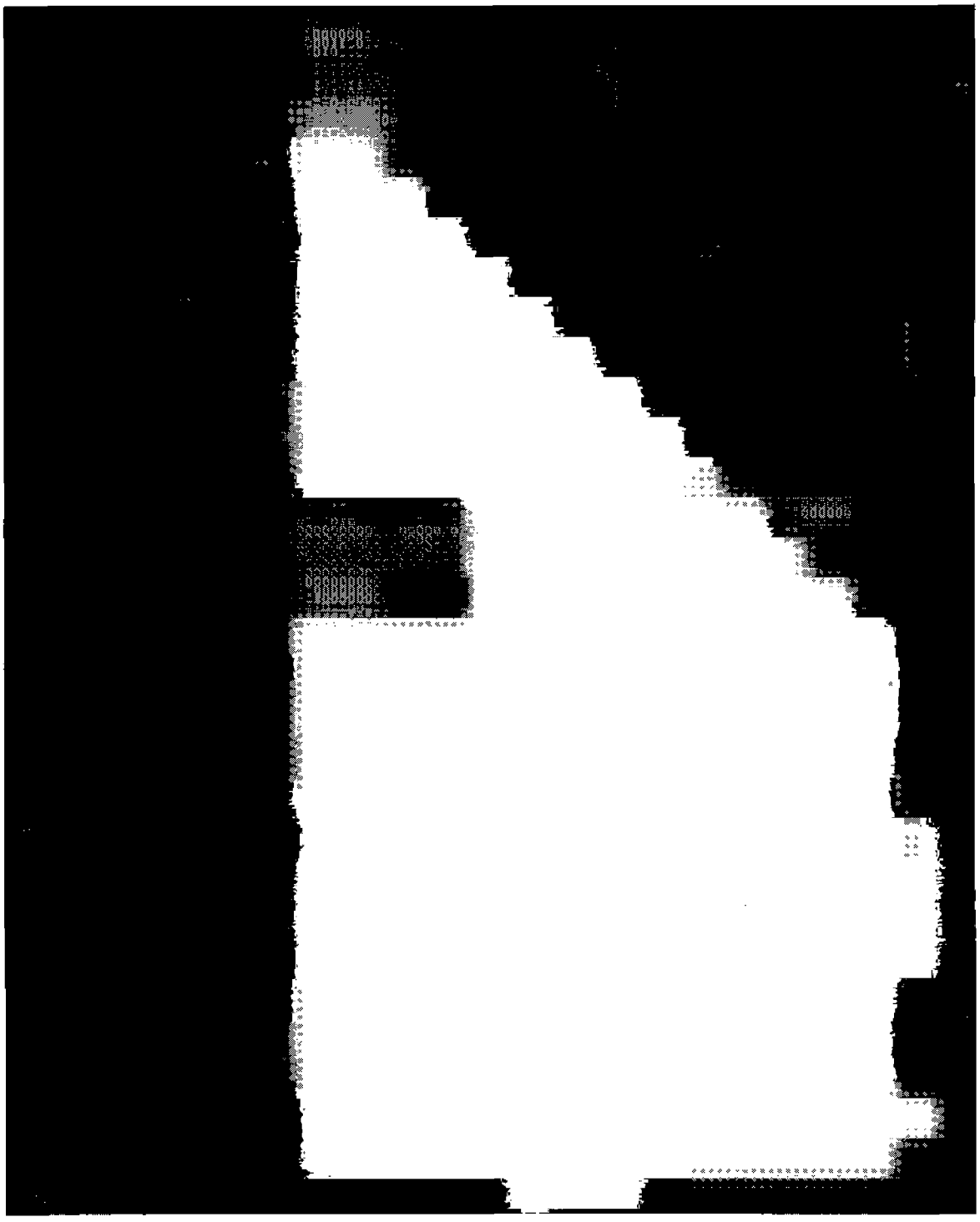


DRAFT
WORKING DOCUMENT

[redacted] Last Updated: 12/7/2006

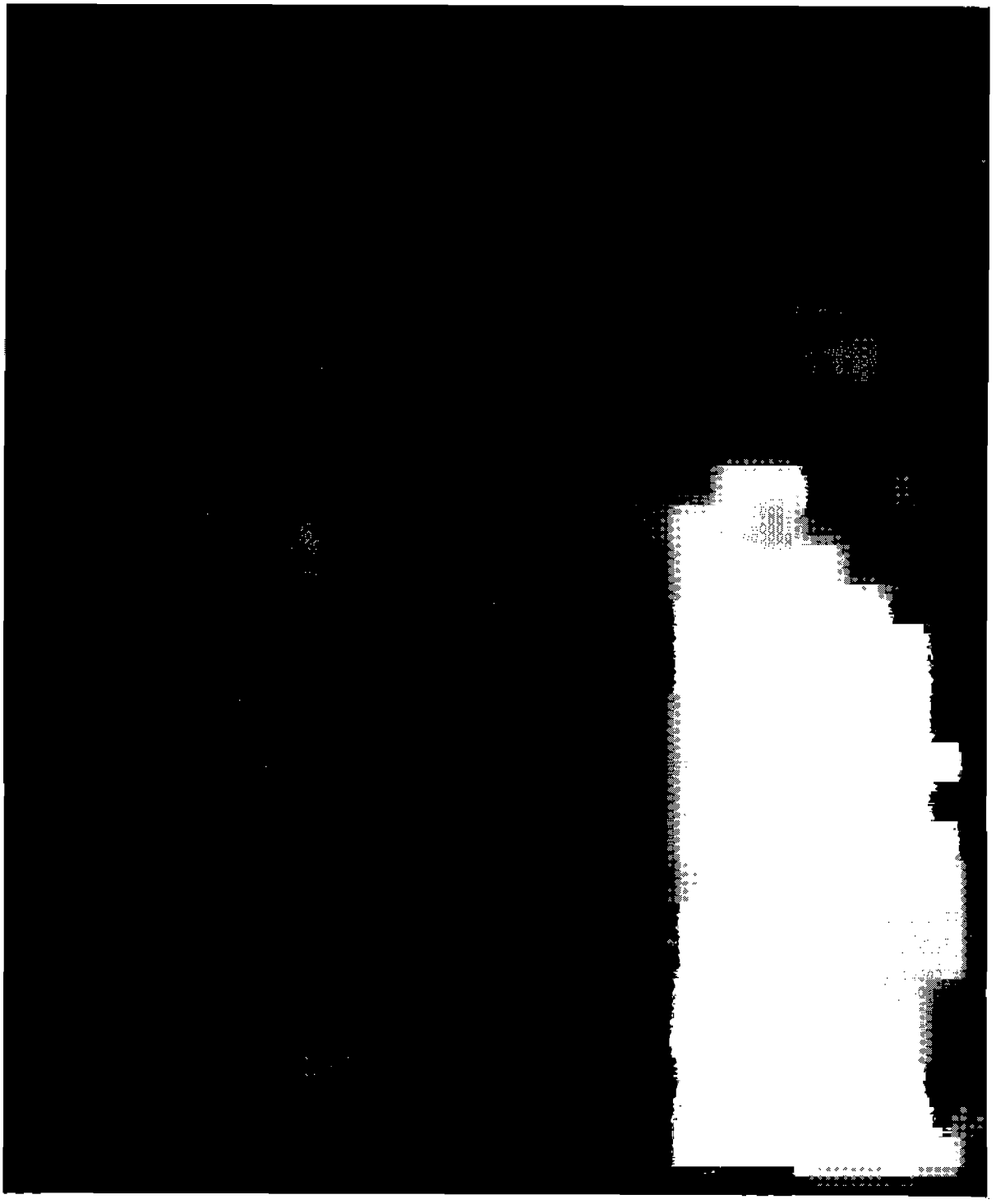


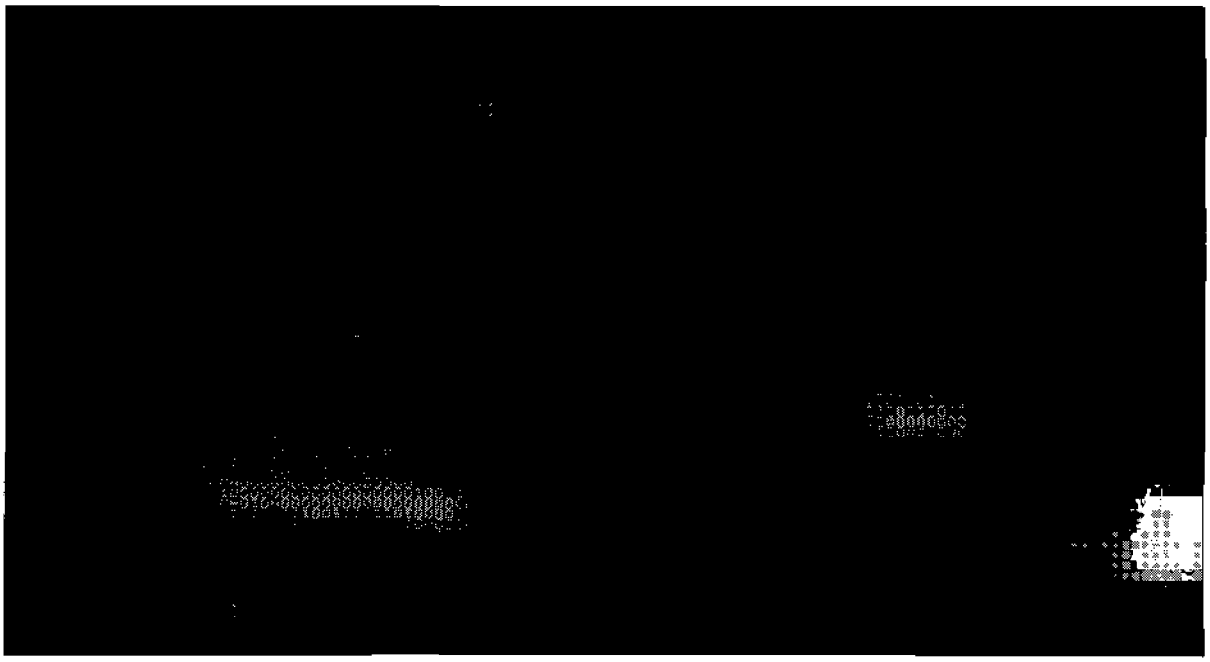
DRAFT
WORKING DOCUMENT

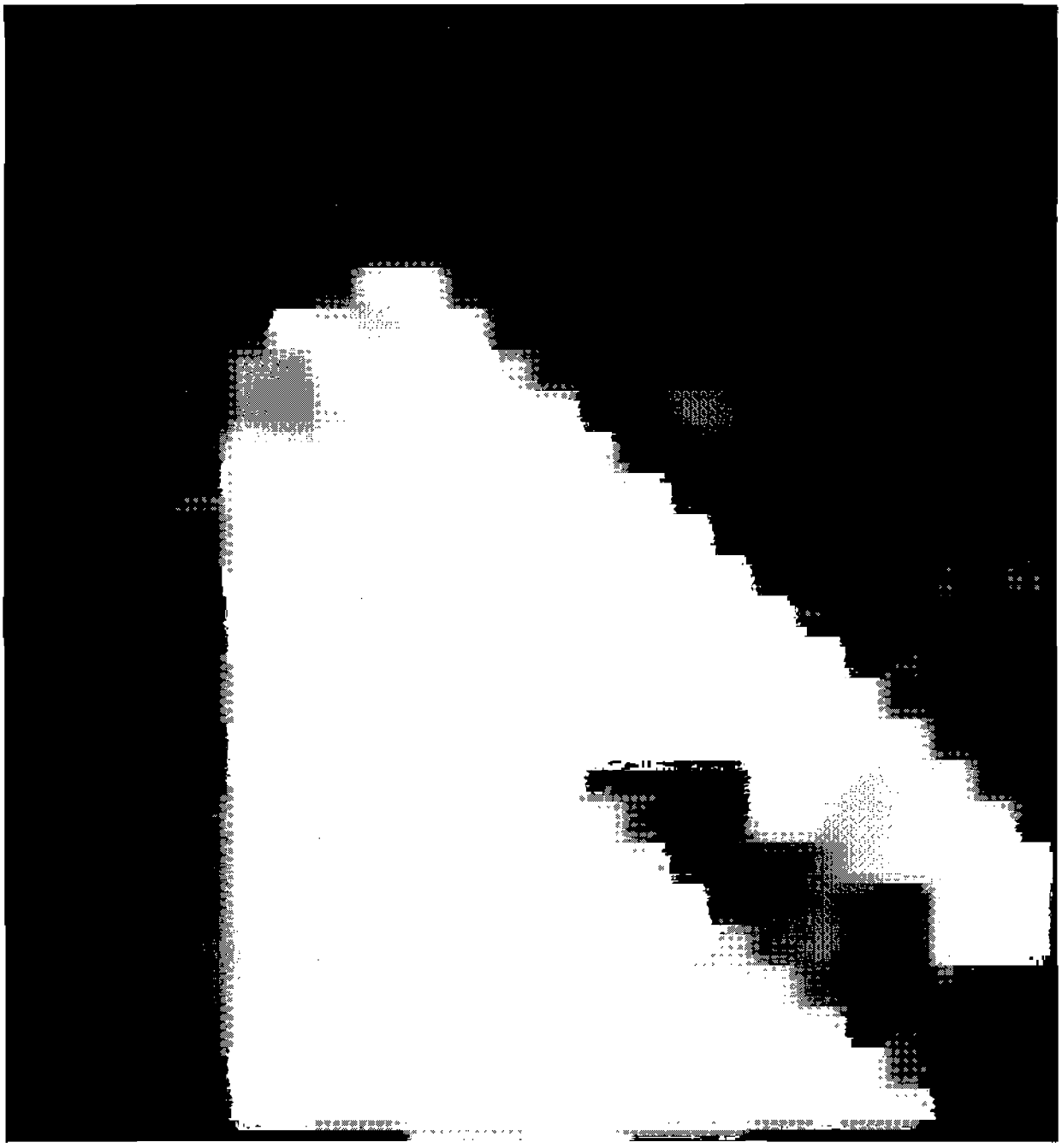


DRAFT
WORKING DOCUMENT

[redacted] Last Updated: 12/7/2006







[redacted] CTR OSD OUSDI

From: [redacted] OSD-NII
Sent: Wednesday, July 13, 2005 10:44 AM
To: [redacted]

Subject: Blogs & Content Security (Automated Monitoring) (FOUO)

FOR OFFICIAL USE ONLY

[redacted]
--
[redacted]
Planning, Policy, and Integration
DASD(DCIO)
Office: [redacted]
Mobile: [redacted]

This may contain information exempt from mandatory disclosure under the Freedom of Information Act (FOIA).

[redacted] **CTR OSD OUSDI**

From: [redacted] CIV OSD OUSDI
Sent: Wednesday, October 05, 2005 1:28 PM
To: [redacted] CTR OSD OUSDI
Subject: FW: FYI Only - Blog Insight (UNCLASSIFIED) (U)

Follow Up Flag: Follow up
Flag Status: Green

UNCLASSIFIED

From: [redacted]
Sent: Wednesday, October 05, 2005 11:52 AM
[redacted]
Subject: FYI Only - Blog Insight (UNCLASSIFIED)

Classification: UNCLASSIFIED

Caveats: FOUO

All,

Blog link which has some good insight into what we□re dealing with, notice the discussion of OPSEC related issues. The blog (1st link) was linked in a FoxNews article (2nd link).

If you□re curious as to the visibility that the CSA□s OPSEC message has received, Google OPSEC [redacted] and check out the results.

http://philandbecky.blogspot.com/

http://www.foxnews.com/story/0,2933,171255,00.html

[redacted]

HQDA G-3, ATTN: DAMO-ODI (Info Ops)

OPSEC Officer

[redacted]

NIPRNET - [redacted]

SIPRNET - [redacted]

Fax [redacted]

Classification: UNCLASSIFIED

Caveats: FOUO

[redacted] CTR OSD OUSDI

From: [redacted] Mr, NII/DoD-CIO
Sent: Thursday, October 12, 2006 3:16 PM
To: [redacted] Mr NETCOM/LMIT
Cc: [redacted] Ms, NII/DoD-CIO; [redacted] USA JTF-GNO J3 [redacted] CTR OSD OUSDI [redacted] OSD-ATL
Subject: RE: Is this a Military site? (UNCLASSIFIED) (U)
Signed By: [redacted]@osd.mil

UNCLASSIFIED

Looks like the last slide provides the contact information for the speaker.

From: [redacted] NII/DoD-CIO
Sent: Thursday, October 12, 2006 2:53 PM
To: [redacted] NETCOM/LMIT
Cc: [redacted] Ms, NII/DoD-CIO; [redacted] USA JTF-GNO J3 [redacted] CTR OSD OUSDI; [redacted] Ms, OSD-ATL
Subject: RE: Is this a Military site? (UNCLASSIFIED) (U)

UNCLASSIFIED

Hi [redacted]

JWRAC has not been abolished as far as I know, but I don't beleive that it is active at this time.

My last POC with JWRAC is [redacted] (cc'd). If he is not with JTF-GNO now, the CDO at JTG-GNO may be able to help - cdo@jtf-gno.mil. [redacted] may have some insight about the status of JWRAC that she can share (cc'd).

I spoke with [redacted] at DTIC about the National Defense Industrial Association ((NDIA), http://www.ndia.org/) (DTIC hosts NIDA related material at www.dtic.mil/ndia/) and she explained that NDIA is not a DoD organization. NDIA is in the business of hosting/coordinating events for DoD. They post material (with the permission of the speaker) that is used at the events they host.

I recommend that you contact the NDIA POC for "Proceedings" [redacted] and ask her to remove the FOUO material. You may also want to ask who gave permission to post it and give them a call to let them know that the NDIA posts material to a publicly accessible website.

Hope this helps, [redacted]

From: [redacted] NETCOM/LMIT
Sent: Thursday, October 12, 2006 2:16 PM
To: [redacted] Mr, NII/DoD-CIO
Subject: FW: Is this a Military site? (UNCLASSIFIED)
Importance: High

Classification: UNCLASSIFIED

Caveats: NONE

*NOTICE: Message body content downgraded from previous markings UNCLASSIFIED//FOUO by [redacted]

Is there anyone still working at JWRAC?

[redacted] (Lockheed Martin)
Web Risk Assessment/Information Assurance Analyst
[redacted]@us.army.mil

From: [redacted] NETCOM/LMIT
Sent: Thursday, October 12, 2006 1:22 PM
To: [redacted] NETCOM/LMIT
Subject: FW: Is this a Military site? (UNCLASSIFIED)
Importance: High

Classification: UNCLASSIFIED

Caveats: FOUO

Hi [redacted]

THis was forwarded to me from [redacted] Is this a site that we can go after or one that we need to leave alone? See the email below.

[redacted]

[redacted]
LMIT Professional Services

Information Assurance Directorate NETC-EST-A

Army Web Risk Assessment Cell
A&VTR Analyst
[redacted]
[redacted]@us.army.mil
AKO IM User

From: [redacted] MEDCOM HQ
Sent: Thursday, October 12, 2006 1:02 PM
To: [redacted] NETCOM/LMIT
Subject: Is this a Military site? (UNCLASSIFIED)

Classification: UNCLASSIFIED
Caveats: FOUO

[redacted]
Is this a military site?
v/r
[redacted]

http://proceedings.ndia.org/exhibits/pdf/6070_martin.pdf#search=%22JIEDDO%20phone%22
<http://proceedings.ndia.org/exhibits/pdf/6070_martin.pdf#search=%22JIEDDO%20phone%22>

Classification: UNCLASSIFIED
Caveats: FOUO