“ILOVEYOU” VIRUS

LESSONS LEARNED REPORT

Assured Information for America's Power Projection Army

FORSCOM

FREEDOM'S GUARDIAN

DCSC4

FORSCOM IAO

DEPARTMENT OF THE ARMY
HEADQUARTERS UNITED STATES ARMY FORCES COMMAND
1777 HARDEE AVENUE SW
FORT MCPHERSON GEORGIA 30330-1062

REPLY TO
ATTENTION OF

AFCI-J

MEMORANDUM FOR

COMMANDERS, CONUSA
COMMANDER, USARC
COMMANDERS, FORSCOM INSTALLATIONS
COMMANDERS, FORSCOM ACTIVITIES/UNITS REPORTING DIRECTLY TO
HQ FORSCOM

SUBJECT: FORSCOM "ILOVEYOU" Virus Lessons Learned Report

1. On 4 May 2000, the "ILOVEYOU" virus spread throughout U. S. Army networks before Department of Defense anti-virus software updates that could detect and remove it were available. Forces Command (FORSCOM) Directorates of Information Management and activities responded quickly to contain the virus but in the process, email service was impacted. The impacts of the "ILOVEYOU" virus and its variants, as reported to the Army Computer Emergency Response Team, are workstations infected - 2258, man-hours lost - 12,010, and an estimated cost of $79.2K.

2. All FORSCOM activities should review their Information Assurance Posture and Information Operations Condition Plans to ensure that procedures are in place to protect information systems and networks and to respond quickly and decisively when threats occur.

3. Points of contact for this report are LTC Nate Perkins, DSN 367-7515, perkinsnw(at)forscom.army.mil and Don LaBonte, DSN 367-6467, labonted(at)forscom.army.mil.

FOR THE COMMANDER:

Encl
as

JULIAN H. BURNS, JR.
Major General, USA
Deputy Chief of Staff for Operations

AQM03-07-2022

CF:
HQDA, DAMO-ZA/SAIS-ZA/DAMI-ZA
COMMANDER, U.S. ATLANTIC COMMAND

INTERNET DOCUMENT INFORMATION FORM

A. Report Title:"IloveYou" Virus Lessons Learned Report

B. Report downloaded From the Internet: April 29 2003

C. Report's Point of Contact: Department of the Army HDQRS United States Army Forces Command Fort Mcpherson, Georgia 30330-1062

D.

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
DTIC-OCA Initials: __JC__ **Preparation Date May 07 2003**

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.

TABLE OF CONTENTS

ANNEX A (EXECUTIVE SUMMARY) TO "ILOVEYOU" VIRUS LESSONS LEARNED REPORT

EXECUTIVE SUMMARY

On 4 May 00 the "ILOVEYOU" Virus, also known as the "Love Bug", originated in the Philippines and wormed its way into government and business E-mail systems around the globe from Australia and Hong Kong westward through Asia, Europe, and the U.S, including throughout HQ FORSCOM and its subordinate commands.

The "ILOVEYOU" Virus spread about 15 times faster than last year's Melissa computer virus. The program's rapid proliferation brought E-mail Systems worldwide to a grinding halt forcing technicians to take hundreds of systems off-line.

The virus was spread through an E-mail attachment designed to propagate the virus message automatically throughout an agency's Global Email Address Directory.

Unsuspecting users who opened the attachment automatically caused the virus to start spreading throughout their agencies' E-mail System. This overloaded E-mail servers and caused technicians to shut down servers to assess what was happening and attempt to fix the problem.

The virus spread throughout Army networks before Army anti-virus software updates that could detect and remove it were available. FORSCOM DOIMs and activities responded quickly to contain the virus but in the process, email service was impacted. The impact of the virus as reported to the Army Computer Emergency Response Team (ACERT) is: workstations infected - 2258, manhours lost – 12,010, estimated cost - $79.2K.

Recommended actions based on the lessons learned include:

- Ensure that procedures are in place for alerting Information Assurance (IA) and network operations personnel on issues related to IA emergencies/network threats 24 hours/day

- Ensure that the OPs community promulgates Information Operations (IO)/Information Assurance (IA) "situational awareness"

- Continue to emphasize and support IA training

- Propose that HQDA designate and resource FORSCOM/USASC as Executive Agent for Army wide network operations and their protection

ANNEX B (SEQUENCE OF EVENTS) TO "ILOVEYOU" VIRUS LESSONS LEARNED REPORT

SEQUENCE OF EVENTS

04 MAY 00

At approximately 0645 Local Time, Headquarters, FORSCOM got the first indication that there was a problem with the FORSNET Network. A message was received from Fort Stewart, GA that several users at Fort McPherson and Fort Gillem had opened enabling the virus to start spreading throughout FORSCOM's 50,000 email subscribers.

By 0755 Local Time, the FORSNET E-mail Server was in overload with virus messages being readdressed and forwarded to other FORSNET subscribers.

FORSNET Technicians realized they had a major problem and were forced to take the FORSNET E-mail Server offline. By shutting down the Server at this point, FORSNET personnel prevented the virus from spreading any further than the "D's" in FORSCOM's Global Address Directory.

At this point FORSNET personnel were still trying to determine what was happening. There was still no official information concerning a problem or a fix.

DCSC4 IA personnel were alerted to the virus threat by a message on a local radio station on the way to work. IA personnel pulled an ACERT Alert off of the ACERT WEB Site. Realizing there was a major problem, DCSC4 FORSNET, Information Assurance, and Information Systems Security personnel concurrently began contacting FORSCOM Installations to alert them of the Virus problem. Since the E-mail system was down, this had to be accomplished by telephone and facsimile.

At 1045 Local Time FORSCOM transmitted an AUTODIN message setting INFOCON BRAVO throughout FORSCOM.

By 1100 FORSNET personnel had received a fix from Symantic and began implementing the fix by scanning servers to eradicate the virus messages.

By 1200 Local Time the fix was validated and FORSNET General Officer E-mail Servers were brought back on line. The remaining Email FORSNET E-mail were also brought back on line approximately 30 minutes later when full service was restored to the Fort McPherson and Fort Gillem community.

At 1555 Local Time the Land Information Warfare Agency (LIWA) transmitted their Information Assurance Vulnerability Alert (IAVA) (A2000-0007 VBS.LOVELETTER Threat) concerning this virus by E-mail.

At 1600 Local Time DCSC4 made the decision to activate the DCSC4 Crisis Action Team to provide 24/7 coverage at HQ FORSCOM. The CAT Team Shift started at 1600 and continued through 0600 Local Time on 9 May 00.

6 MAY 00

At 1338 Local Time on 6 May 00 DCSC4 personnel transmitted FORSCOM's required acknowledgement of ACERT's IAVA alerting message.

At 1643 Local Time LIWA transmitted an update to it's previous IAVA Alert Message via E-mail.

At 1953 Local Time FORSCOM transmitted an AUTODIN message clarifying and amplifying its earlier INFOCON BRAVO implementation message.

9 MAY 00

At 0600 DCSC4 made the decision to deactivate the DCSC4 Crisis Action Team at HQ FORSCOM.

18 MAY 00

At 1020 Local Time FORSCOM transmitted its 171826Z MAY 00 message downgrading FORSCOM INFOCON to ALPHA. This message also reminded subordinates that a Daily SITREP is still required along with a requirement to provide a Lessons Learned Report NLT 2 Jun 00.

At 1224 Local Time LIWA changed MACOM suspense for MACOM Interim Reports to 191399Z MAY 00.

<u>19 MAY 00</u>

At 1200 Local Time DCSC4 personnel transmitted FORSCOM's Interim A2000-0007 Report to ACERT.

At 1411 Local Time LIWA transmitted its IAVA A2000-0007 Update #2 via E-mail.

<u>24 MAY 00</u>

DCSOPS, DCSC4, and DCSINT conducted a initial 'ILOVEYOU" Virus Hotwash Meeting. This meeting was a free exchange of information concerning the events that happened on 4 May 00.

<u>30 MAY 00</u>

DCSOPS, DCSC4 and DCSINT conducted a second "ILOVEYOU" Virus Hotwash Meeting to prepare a coordinated Hotwash Briefing for DCSC4.

<u>31 MAY 00</u>

DCSOPS, DCSC4, and DCSINT presented its initial "ILOVEYOU" Hotwash Lessons Learned Briefing for DCSC4.

ANNEX C (RECOMMENDATIONS) TO "ILOVEYOU" VIRUS LESSONS LEARNED REPORT

RECOMMENDATIONS

1. General. An issue common to most installation lessons learned reports was the lack of a timely alert. Most FORSCOM installations do not man the network 24 hours/day and the means FORSCOM activites reported first finding out about the virus threat include the following: DOIM network operations noticed increased activity on the emailserver, users reported virus on their workstation, ACERT web page, telephone call from RCERT, JTF-CND web page, national news (e.g., CNN), notified by other units (e.g., 5th SIG called ASC ANSOC). The Information Assurance Vulnerability Alert (IAVA) is a well-documented process with specific responsibilities for the ACERT, MACOM and system administrators at the installations (see TAB I). However, in the case of the "ILOVEYOU" virus, the virus spread throughout Army networks prior to the availability of anti-virus software definition files and many network managers took the emailservers offline to prevent the virus from spreading further. As a result, IA managers and system administrators were not able to get information from the ACERT Listserver which is the primary means of distributing alert guidance.

2. Recommendations

a. Ensure that the OPS community promulgates Information Operations (IO)/Information Assurance (IA) "situational awareness." The network threat spread from east to west and was being worked in Europe prior to activities in CONUS finding out about it. ACERT must analyze the threat and is deliberate in posting alerts. There was no information regarding this threat flowing through OPS channels (e.g., USAREUR, HQDA, JFCOM, FORSCOM) and as a result, most activities were not aware of the threat until approximately 0700 local time.

b. Corps/Div/Bde G3 develop and implement Information Operations SOP IAW FM 100-6 and FM 24-7. Network security and the status of networks is an integral part of IO. A comprehensive SOP would ensure that there was an interface between the G3s and DOIM network operations and that dynamic network situational awareness is established.

c. Establish procedures for ASC's Army Network and Systems Operation Center (ANSOC), Regional Computer Emergency Response Team (RCERT) and FORSCOM installations and commands to contact HQ FORSCOM regarding IA emergencies/network threats 24 hours/day. This is probably best done through the FORSCOM Watch Team. Contact guidance will be developed for FORSCOM activities/RCERT and POCs will be provided to the Watch Team. This also has the benefit of getting the information immediatedly into OPs channels.

d. Refine process for disseminating urgent IA information to DOIMs and IA managers. This is required when the IAVA process is not functioning.

e. Continue to emphasize and support IA training (see ANNEX J).

f. Continue to implement IA tools (e.g., Anti-Virus software, firewalls, proxy servers, intrusion detection systems) to enhance network security.

g. Organize an IO cell with elements from DCSOPS, DCSINT and DCSC4. This would provide a forum to discuss IO/IA issues and would also function as a crisis response cell.

(1) DCSOPS Role

(a) Make decisions regarding the prioritizations of networks and resources

(b) Determine operational impact throughout the command

(c) Oversee Information Operations

(d) Direct subordinate units

(2) DCSINT Role

(a) Provide threat analysis

(b) Analyze incident against world events

(3) DCSC4 Role

(a) FORSCOM proponent for Computer Network Defense (CND)

(b) Manage the FORSCOM Information Assurance program to include development of resource requirements (see TAB K)

(c) Administer FORSCOM MACOM IAVA responsibilities (see ANNEX I)

(d) Advise DCSOPS on issues related to systems and networks

3. ASC Recommendations (see ANNEX D)

a. FORSCOM/USASC must be assigned Executive Agent responsibilities for Army wide network operations and their protection

b. The Army must establish a USR type, standardized reporting system which reflects the "readiness" of Army networks and information systems and the operational impact of not being "ready" or of being under attack. As part of this initiative the Army must redefine which network and systems capabilities must be centrally monitored and reported on by FORSCOM/USASC Theater Network, Systems and Security Operations Centers.

c. FORSCOM/USASC must establish a global, centralized, and fully functional Army Network, Systems and Security Operations Center to provide the Army leadership the Army-level situational awareness and capabilities. This capability would augment ARFOR JTF CND capabilities by providing COMARFOR the Army level information required to execute the CND mission. This service-level network systems and security center would be on the same operational level as the LIWA/ACERT.

d. HQDA must establish requisite funding lines in the budget and POM, and resource approved requirements via FORSCOM funding channels. USASC, through FORSCOM, could then develop, submit, and execute the requisite resource requirements to accomplish the EA mission tasking in the Planning, Programming, and Budgeting Execution System (PPBES).

ANNEX D (COMMANDER ASC PERSPECTIVE) TO "ILOVEYOU" VIRUS LESSONS LEARNED REPORT

COMMANDER ASC PERSPECTIVE

1. Recent events such as the "I LOVEYOU" virus again demonstrate that the Army must aggressively move to implement a rigorous and comprehensive defense-in-depth of our networks and critical systems. Reporting delays and the unavailability of critical, timely data highlight procedural and technical shortfalls with the Army's current "hasty" defense of its information systems and networks. Had the virus been more lethal(something we can expect will occur with greater frequency), these shortfalls could have precluded the development, coordination and execution of adequate response measures. We cannot afford the increasing risks of continuing in this already thin defensive posture. Strengthening existing USASC and ACERT capabilities, enforcing and exercising standardized procedures and clearly defining roles and responsibilities will help ameliorate these shortfalls.

2. In 1998, the VCSA assigned FORSCOM/USASC the mission to perform intrusion detection functions and worldwide network monitoring as part of its existing core mission of operating, protecting, and maintaining networks and providing network and systems management. These initial capabilities have successfully been implemented in the CONUS and OCONUS theaters as part of the first phase of the Army's Network Security Improvement Program (NSIP). OCONUS, USASC Commanders, dual hatted as the MACOM G6, provide the single focal point for all theater reporting and technical direction, consistent with the principles of unity of command. However, the Army has yet to give FORSCOM/USASC the mission, responsibility and authority required to execute centralized technical oversight and direction of the Army's networks, along with the charter to direct the network operations and accompanying reporting procedures for CONUS MACOMs and their installation networks. In addition, USASC lacks the resources to centrally execute a comprehensive, fully integrated, global situational awareness of Army networks and critical information systems. Fixing these shortfalls would provide the Army a single focal point for the health of ALL Army networks and systems and provide the ability to rapidly disseminate and implement standardized reporting procedures and formats. Such a capability would also provide the ARFOR CND JTF a single entry point for the reporting, direction and coordination of responses to computer incidents. Clearly, these are essential elements to a successful, unified defense in-depth.

3. From a USASC perspective, the solution requires multiple actions.
First, FORSCOM/USASC must be assigned Executive Agent responsibilities for Army wide network operations and their protection. This mission should include but not be limited to:

a. Programming, planning, implementing and executing Armywide actions supporting the operational perimeter security for Army networks (to include intrusion detection devices), and the security of designated critical systems.

b. Design, with CECOM coordination, and control access into Army networks and the Army DMZ (that portion of the Army installation networks which controls external access to Army information technology assets on the Army installation), i.e., the top level architecture.

c. Protecting the Army SIPRNET/NIPRNET services (classified and unclassified), i.e., the Army domain name system (DNS), the Army's proxy web caching engines, the terminal server access controller system (TSACS), etc.

d. Providing technical guidance and operational engineering for Army networks and associated services.

e. Providing centralized worldwide situational awareness, operational status and reporting of Army networks and critical systems.

f. Execute centralized configuration management associated with hardware and software for all of the above functions.

4. Second, HQDA must establish requisite funding lines in the budget and POM, and resource approved requirements via FORSCOM funding channels. USASC, through FORSCOM, could then develop, submit, and execute the requisite resource requirements to accomplish this mission tasking in the Planning, Programming, and Budgeting Execution System (PPBES). MACOMS should retain responsibility for programming of IA within their areas of responsibility (below the DMZ). And, MACOMS should assist in funding IA resource requirements within the DMZ until such time as a formal, centralized funding line is established by HQDA.

5. Third, the Army must establish a USR type, standardized reporting system which reflects the "readiness" of Army networks and information systems and the operational impact of not being "ready" or of being under attack. As part of this initiative the Army must redefine which network and systems capabilities must be centrally monitored and reported on by FORSCOM/USASC Theater Network, Systems and Security Operations Centers. Today, we have the mission and the resources to monitor only a selected number of Army defined critical systems. For example, all Army critical email services are not centrally monitored.

6. Fourth, to fully integrate Army network operations, FORSCOM/USASC must establish a global, centralized, and fully functional Army Network, Systems and Security Operations Center to provide the Army leadership the Army-level situational awareness and capabilities described in paragraph 2 above. This capability would augment ARFOR JTF CND capabilities by providing

COMARFOR the Army level information required to execute the CND mission. This service-level network systems and security center would be on the same operational level as the LIWA/ACERT. My staff is developing a concept plan with resource impacts for this proposal, with the guidance to capitalize existing assets to the greatest extent possible. I have suspensed my staff to have the first cut of this concept plan ready for your review within 30 days, to include a first cut estimate of resources required. The exact resource requirement to implement plan will take a bit longer based on coordinate to be done with other than FORSCOM elements, but will be completed soonest. If you concur with concept plan, we should finish fleshing out the $ requirement, get the boss' (DCG & CG) approval and then push to HQDA.

7. Bottomline: FORSCOM is simply not missioned or structured to do the in-depth, permanent network defense the Army leadership expects and deserves. We cannot afford to continue to "band-aid" this critical area of operations.

ANNEX E (SUMMARY OF IMPACT) TO "ILOVEYOU" VIRUS LESSONS LEARNED REPORT

A2000-0007 FORSCOM Final Report - ILOVEYOU Virus & Variants

INSTALLATION	AV Product	# Networks	# Computers	OS	Impact	Damage	Source	Lost	# Files	Estimated
		Infected	Infected					Manhours	Infected	Costs - $
BRAGG	Norton	1	380	Win95,98, NT	Recovered	Reload	Email	1400	204,798	15000
CAMPBELL	Norton	1	52	Win95,98,NT	Recovered	Minor	Email	850	Unk	4000
CARSON	Norton	1	17	Win NT	Partial	Minor	Email	525	72,500	2500
DRUM	Norton/McAfee	1	83	win3.1,95,98,NT	Recovered	Rebuild	Email	1300	Unk	4500
HOOD	Symantic	1	152	Win 95, 98, NT	Recovered	Minor	Email	1550	4650	20000
IRWIN	Norton	1	90	Win95,98, NT	Unk	Minor	Email	800	Unk	1600
LEWIS	Norton	1	89	Win95,98,NT	Partial	Rebuild	Email	1100	Unk	6800
MCPHERSON	Norton	3	925	Win95,98,NT	Recovered	Rebuild	Email	1400	4050	7000
POLK	Norton/McAfee	1	70	Win95,98,NT	Partial	Rebuild	Email	1,300	Unk	2100
RILEY	Norton	1	280	Win95,98, NT	Unk	Rebuild	Email	1135	115,332	4000
STEWART	Norton/McAfee	1	120	Win95,98,NT	Unk	Rebuild	Email	650	Unk	11700
TOTALS:		**13**	**2258**					**12010**		**79,200**

Information depicted above was provided by Installation IAVA POC and represents reports as of 311200MAY2000.

Lost Manhours do not include lost user productivity.

Files Infected: Most installations were unable to capture accurate statistics in this area.

Estimated Costs: This includes known costs for overtime and equipment / software purchases.

ANNEX F (INSTALLATIONS' LESSONS LEARNED) TO "ILOVEYOU" VIRUS LESSONS LEARNED REPORT

INSTALLATION LESSONS LEARNED

APPENDIX 1 (FORT BRAGG) TO ANNEX F (INSTALLATIONS" LESSONS LEARNED) TO "ILOVEYOU" VIRUS LESSONS LEARNED REPORT

FT BRAGG

AV Product	# Networks	# Computers	OS	Impact	Damage	Source	Lost	# Files	Estimated
	Infected	Infected					Manhours	Infected	Costs - $
Norton	1	380	Win95,98, NT	Recovered	Reload	Email	1400	204,798	15000

6a. When and how did you find out about the virus? Virus was noted by several e-mail users when they arrived for work on the morning of 4 May.

6b. What actions did you take and what were the results?

1. Blocked the web site. Firewall enabled us to identify the IP addresses and disabled infected users accounts. Infected computers were disconnected from the network and conducted cleanup operations.

2. Fort Brag programmers analyzed the scrip of the virus and with additional information gathered from other sources at ACERT and RCERT created and utilized a virus removal tool until an official version wasreleased by ACERT.

3. Stopped the IMS to prevent additional incoming/outgoing traffic. Stopped the MTA's and began scanning and deleting the subject line. Deleted in excess of 300,000 potential launches.

4. Sent a notification to all users to delete anything that may have been in the queue, inbox, personal folders, and deleted items, pending receipt of signature updates. This action allowed us to handle internal mail during cleanup activities.

5. Posted on Intra Web site the virus signature and clean instructions upon receipt from ACERT and sent notification to all e-mail recipients on the installation to update of their systems.

6. Restricted IMS e-mail to 7KB to allow basic e-mail in and out of the installation. This action minimized risk of re-infection from external agencies.

7. Provided information to IMOs/ISSOs upon receipt to keep ahead of variants. Reminded all e-mail recipients to delete anything suspicious to minimize the possibility of re-infection.

8. Updated the Virus Scan software on exchange servers upon receipt from ACERT.

9. Captured additional IPs hitting firewall, and user ids from dial-in systems. Conducted final cleanup activities.

6c. What support did you receive from ACERT/RCERT/ANSOC? Was this support timely? Virus removal instructions with step-by-step instructions were published by ACERT and trained anti virus personnel were available foractivities that required assistance. Yes, support was timely.

6d. What support did you need but did receive? A pre-warning should have been issued when the virus problem first began prior to it hitting the installations. The Intranet site should have been blocked at the egress points to the Internet when first identified. These action would have saved a lot of headaches for other installations.

6e. What are your recommendations on how future attacks should be handled? Be reactive initially.

6f. What support can HQ FORSCOM provide that would help you in these situations? Highly recommend proxy agents at Internet connections for tighter control, or a more responsive approach to overall infrastructure protection, even if the problem appears to be isolated - it probably isn't considering the speed of data transmission.

Randy Cantrell
Security Officer/C2Protect POC
Information Technology
Business Center
910 396-8752/DSN 236-8752
FAX 910 396-5499/DSN 236-5499

APPENDIX 2 (FORT CAMPBELL) TO ANNEX F (INSTALLATIONS" LESSONS LEARNED) TO "ILOVEYOU" VIRUS LESSONS LEARNED REPORT

FT CAMPBELL

AV Product	# Networks	# Computers	OS	Impact	Damage	Source	Lost	# Files	Estimated
	Infected	Infected					Manhours	Infected	Costs - $
Norton	1	52	Win95,98,NT	Recovered	Minor	Email	850	Unk	4000

6A. WHEN AND HOW DID YOU FIND OUT ABOUT THE VIRUS?
When we came in at 0815 and a Majordomo message with a time group of 0615 was waiting for me. Recommendation: Because not all operations are 24/7 If a significant message such as this virus alert, notification of the Division SDO would have been more prudent. This would have given us at least 3 more hours to react, and may have cut down our infection rate considerably. Because some people come in early and do their e-mail we have identified approximately 57 infected senders of which approximately 15 were from off post sending the virus. We had over 15000 I love you messages cleaned off the exchange servers. By earlier notification this may have been significantly lower.

6B. WHAT ACTIONS DID YOU TAKE AND WHAT WERE THE RESULTS.
Went into the server room and shut down all the e-mail services. The results were e-mail on fort Campbell was down for approximately 32 hours while we cleaned up our servers and scanned all files.

6C. WHAT SUPPORT DID YOU RECEIVE FROM ACERT/RCERT/ANSOC?
WAS THIS
SUPPORT TIMELY?
The support we received from ACERT was helpful in the beginning but as the virus progressed it seemed as if ACERT was overwhelmed. Also when Symantec (on their site) had a cleanup fix for the virus, the ACERT site continued evaluating it for more than 48 hours. We were "cleaned" and back on line before ACERT posted any fixes.

6D. WHAT SUPPORT DID YOU NEED BUT DID NOT RECEIVE?
Timely updates, unable to reach any of the Key personnel at FORSCOM because they were literally flooded with requests for information and guidance and or in meetings determining the best courses of action. No "body" was available to answer questions.

Recommendation: Have a central point of contact with both telephone and fax numbers so that if e-mail services are shutdown there are alternate means of communication, and make sure this information is disseminated to all security managers and alternates. This would insure that there is a communication path available even if a unit is proactive and brings their site down because of a threat or other disaster.

APPENDIX 2 (FORT CAMPBELL) TO ANNEX F (INSTALLATIONS" LESSONS LEARNED) TO "ILOVEYOU" VIRUS LESSONS LEARNED REPORT

6E. WHAT ARE YOUR RECOMMENDATIONS ON HOW FUTURE ATTACKS SHOULD BE
HANDLED?

1. Establish notification process that includes Division or Corps SDO or the point of contact provided by the local installations for after duty hours emergencies.
2. Provide central point of contact that is available and include both FAX and Telephone numbers at Forces Command and man them.
3. Insure that that the notification processes during duty hours includes the Security manager and alternates with their phone numbers and Faxes.

6F. WHAT SUPPORT CAN HQFORSCOM PROVIDE THAT WOULD HELP YOU IN THESE
SITUATIONS?

The comment was made to check your SMS system. Unfortunately we don't have SMS and have not been funded to receive it. We are being funded for Tivoli down to the server level but if tivoli is going to be the standard it should be funded to the user level to provide continuity of operations.

Funding to bring all machines to an operating systems level of NT or Windows 2000. This would help to standardize operations and programs.

POCS Jim Cunningham (DSN 635-7448), Dan O'Brien (DSN 363-4449)

APPENDIX 3 (FORT CARSON) TO ANNEX F (INSTALLATIONS" LESSONS LEARNED) TO "ILOVEYOU" VIRUS LESSONS LEARNED REPORT

FT CARSON

AV Product	# Networks	# Computers	OS	Impact	Damage	Source	Lost	# Files	Estimated
	Infected	Infected					Manhours	Infected	Costs - $
Norton	1	17	Win NT	Partial	Minor	Email	525	72,500	2500

WHEN AND HOW DID YOU FIND OUT ABOUT THE VIRUS? The DOIM received a voice mail notification from FORSCOM 0600 hours. Note: SA's noticed an increase in message activity at 0630. Official notification through AUTODIN message was received approx. 1100 hours.

WHAT ACTIONS DID YOU TAKE AND WHAT WERE THE RESULTS? E-mail servers were shut down. Waited for a Norton AV update. Updates were installed and Manual Scans of individual mail boxes were activated. Systems were brought on- line as soon as we were assured the NAV was detecting the virus and their mail box was clean. Notifications went out to all users with instruction on what to do with suspect messages/files. Changed the log-on script to notify users of the threat and what to do. The DAA directed that infected workstations be removed from the network. Commanders would have to inform the DAA to have a user re-activated. Results: the warning script helped. CNN reports validated the severity of the attack. DAA orders pushed the responsibility to the user and it was of great value. it is very hard to measure preventative proactive actions. bottom-line is the user must be made aware and informed on what action to take.

WHAT SUPPORT DID YOU RECEIVE FROM ACERT/RCERT/ANSOC? No support was received. Called ACERT and they just provided a possible time line when the Norton AV maybe available, already had the information provided by the local news media. They did provide a of minimum support, after ACERT received the Norton AV update, they posted it to their website. This was positive because Norton was flooded with requests. But they did not tell anybody. WAS THIS SUPPORT TIMELY? No, in general. Okay as far as posting the information. Do not believe these organizations are staffed to provide support. The best they can do is report history. There is a very real need to develop a CND team somewhere -- CINCSPACE! They could use a redundant commo system to provide resolution to situations.

WHAT SUPPORT DID YOU NEED BUT DID NOT RECEIVE? Timely notification through the Emergency Operations Centers which has 24x7 manning and emergency notification instructions would have provided more reaction time. this way activities would have a little time to take control and influence damage control, like re-writing the log-on script or shutting down the system before users report for duty. this is especially true for weekends and holidays. ACERT and DISA should notice activity in Europe before it hits CONUS just based on time zones. until you can get inside the decision cycle you will not control the situation. Consider looking at the Y2K contingencies and implementing the "best practices theory".

WHAT ARE YOUR RECOMMENDATIONS ON HOW FUTURE ATTACKS SHOULD BE HANDLED?
We need to have a push package originating out of each RCERT, as to not overload the ACERT. if this is considered an IO type of attack then the guidance(push a canned warning log-on script) and what can the installation's expect in the way of support (who, what and When). leaders need basic information to develop a course of action, without guidance everyone is on their own. if this is what it is going to be then tell us up front. warnings needs to flow from OPS side as well as G6. it could be a coordinated message. this is a "GREEN TAB ISSUE". RCERTS need to establish a notification and communication net separate from the general service system. this will be used to push fixes and guidance without having to deal with the confusion on the general service system. consider using the SIPRNET pipe for guidance. Even a RAS (RADIUS) could be established to pass information other than relying on your clogged gateway. SOP to isolate your LAN by installation needs to be in place. then use the other means (above) to communicate. there are no redundant circuits.

WHAT SUPPORT CAN HQ FORSCOM PROVIDE THAT WOULD HELP YOU IN THESE SITUATIONS? See the above comments. FORSCOM needs to push the "GREEN TAB ISSUE". Commanders need to be involved. The combat support systems theyare relying on will not be readily available under IO/ CNA conditions. The Army does not have the luxury to wait 3-4 years to field a new system in today's rapidly changing technical and political environment. It only takes one insider or someone with a computer and the knowledge to launch an attack. if you are relying on power projection platforms to provide the resources for a deployment then they need to be protected accordingly. We need bodies and dollars to pay the people to manage and control the systems.

OUR EOC CONTACT NUMBERS: 719-526-3400 (PRIMARY)

719-526-5914 (ALTERNATE)

719-526-5825 (FAX)

OUR DSN IS PREFIX 691-XXXX

V/R

Jim Preston

APPENDIX 4 (FORT DRUM) TO ANNEX F (INSTALLATIONS" LESSONS LEARNED) TO "ILOVEYOU" VIRUS LESSONS LEARNED REPORT

FT DRUM

AV Product	# Networks	# Computers	OS	Impact	Damage	Source	Lost	# Files	Estimated
	Infected	Infected					Manhours	Infected	Costs - $
Norton/McAfee	1	83	win3.1,95,98,NT	Recovered	Rebuild	Email	1300	Unk	4500

6A. WHEN AND HOW DID YOU FIND OUT ABOUT THE VIRUS?
May 4th at approximately 7:00 am. The e-mail service was extremely slow. It was noted that a high profile individual on post had sent a message to several people with "I Love You" in the subject area of the memo. A member of the network security team called the ACERT and a answer phone took their message. Another call was made to the RCERT and they alerted us to the situation.

6B. WHAT ACTIONS DID YOU TAKE AND WHAT WERE THE RESULTS.
A decision was made to block all traffic coming into and out of post on port 25 until we could get a handle on the situation. The result being that the e-mail server did not crash. We were able to get a handle on the situation instead of just reacting.

6C. WHAT SUPPORT DID YOU RECEIVE FROM ACERT/RCERT/ANSOC? WAS THIS
SUPPORT TIMELY?
We made several calls to the RCERT for updates and guidance. We made several calls to the ACERT for guidance and updates. The support was as timely as it could be. Both agencies were trying to figure out the extent of the damage and all options

6D. WHAT SUPPORT DID YOU NEED BUT DID NOT RECEIVE?
Because of the nature of the issue we probably got all the support we could.

6E. WHAT ARE YOUR RECOMMENDATIONS ON HOW FUTURE ATTACKS SHOULD BE
HANDLED?
The guidance on were to go (web sites, agencies) and what is the bottom line on actions we have to take. For instance, what agency we take direction from when there is conflicting information (RCERT, ANSOC, ACERT, FORSCOM).
At one point, a fix came out for the virus one agency told us it was available and the other said that we couldn't use it.

The first action that should be taken is block all traffic (ports relative to the attack) to the critical server to prevent it from crashing, isolate it from the network and block any IP's that may try to penetrate the network based on the situation. Depending on the OS involved and the type of attack other critical servers that could be effected should be protected immediately.

6F. WHAT SUPPORT CAN HQFORSCOM PROVIDE THAT WOULD HELP YOU IN THESE
SITUATIONS?

Keep us informed. For the first two days we really didn't have any guidance. On the following Monday May 8th, we were finally instructed to receive our guidance from the ACERT's web page regarding updates and pertinent information.

APPENDIX 5 (FORT HOOD) TO ANNEX F (INSTALLATIONS" LESSONS LEARNED) TO "ILOVEYOU" VIRUS LESSONS LEARNED REPORT

FT HOOD

AV Product	# Networks	# Computers	OS	Impact	Damage	Source	Lost	# Files	Estimated
	Infected	Infected					Manhours	Infected	Costs - $
Symantic	1	152	Win 95, 98, NT	Recovered	Minor	Email	1550	4650	20000

1. WHEN AND HOW DID YOU FIND OUT ABOUT THE VIRUS?

The DOIM Virus POC checks the RCERT and commercial web pages daily prior to 0730 for information concerning new viruses. The virus POC learned about the virus through various commercial virus information web services and notified the chain of command at approximately 0705, 4 May 00.

2. WHAT ACTIONS DID YOU TAKE AND WHAT WERE THE RESULTS?

The DOIM Virus POC immediately sent out an e-mail to the Fort Hood IMOs warning them of this virus. This action resulted in users currently on the Fort Hood ILAN being informed of the virus prior to the ILAN being taken out of service.

The Fort Hood email servers were taken out of service at 0730 to prevent the spread of the virus. Once the new anti-virus was received from Symantic the servers were loaded with the changes and brought back on line. The e-mail servers were returned to service at approximately 1600, 4 May 00. During the time the servers were down, the ISSM contacted Fort Hood AISSMs via telephone and provided guidance on what was to be passed to all users to stop the spread of the virus once the e-mail servers were brought back into service. The DOIM operations officer held a meeting with all key personnel to discuss what had occurred, what actions had been taken to date, what future action was required to prevent the spread of the virus and what measures were required to ensure the Fort Hood email servers remained operational. Several virus information e-mail messages were released by the Virus POC, the ISSM and the CDR 1114th Signal Battalion to all levels of command providing guidance on procedures to be followed if you had an infected computer and instructions on how to prevent the spread of the virus. Over the course of the next few days, several times each day as information concerning this virus was received it was passed out to the AISSMs, IMOs ISSOs and Battalion Commanders on Fort Hood.

As new infections developed the e-mail team immediately contacted the user of the system that was spreading the virus. The ISSM was also informed by the e-mail team and immediately contacted the AISSM of the user with infected computer to ensure this system was in fact disconnected from the network and the AISSM filed the required virus report.

IMOs and ISSOs on Fort Hood personally checked each machine in their area of responsibility to ensure the most current version of anti-virus was loaded and systems were not infected rather than rely on individual users to perform this task.

Soldiers were provided information at morning formation concerning this virus and precautions to take if the infected e-mail was received.

To ensure there is no one who has not been advised of what precautions to take against this virus, all AISSMs have been instructed to contact personnel who are deployed, on leave or TDY. Over the course of the next couple of weeks, over 2,000 soldiers from the 1CAV will be returning to Fort Hood from NTC. An IA representative from 1CAV will provide a virus prevention briefing to arriving soldiers prior to their departing the airfield.

Soldiers on Fort Hood, because of Physical Training (PT) requirements, do not report for work until 0900 on Monday, Wednesday, and Friday. The fact that not all users were on the system when the virus first arrived and majority of users were informed of virus precautions prior to the system coming back up contributed greatly to the low number of infected computers on Fort Hood. This in combination with all of the above actions resulted in a very low number of ILOVEYOU infections on Fort Hood.

3. WHAT SUPPORT DID YOU RECEIVE FROM ACERT/RCERT/ANSOC? WAS THIS SUPPORT TIMELY? In most cases information concerning the virus was available on commercial virus web pages hours before ACERT made it available to us. The Fort Hood Virus POC was in contact with ACERT several times asking questions about the development of a fix or a patch to prevent the virus. Patches were provided to us from ACERT that had not been tested by them. Fort Hood was asked to load these patches and then provide results of the patches performance back to the ACERT. For the most part ACERT was very helpful and timely with answering our questions.

4. WHAT SUPPORT DID YOU NEED BUT DID NOT RECEIVE?

Timely notification of the virus attack, information about the virus, and information concerning the development of a fix or patch.

5. WHAT ARE OUR RECOMMENDATIONS ON HOW FUTURE ATTACKS SHOULD BE HANDLED?

ACERT should notify the MACOM's immediately. The MACOM's should notify the installations via Command Channels using the Operations Centers.

6. WHAT SUPPORT CAN HQFORSCOM PROVIDE THAT WOULD HELP YOU IN THESE SITUATIONS?

Timely Notification through the FORSCOM Operations Center (FOC) to the installation operations centers.

Minimal Reporting Requirements.

APPENDIX 6 (FORT IRWIN) TO ANNEX F (INSTALLATIONS" LESSONS LEARNED) TO "ILOVEYOU" VIRUS LESSONS LEARNED REPORT

FT IRWIN

AV Product	# Networks	# Computers	OS	Impact	Damage	Source	Lost	# Files	Estimated
	Infected	Infected					Manhours	Infected	Costs - $
Norton	1	90	Win95,98, NT	Unk	Minor	Email	800	Unk	1600

When and how did you first find out about the virus?

Telephonic and E-mail alert from FORSCOM and a Virus Alert from ACERT on same day of virus attack.

What actions did you take and what were the results?

E-Mail server was taken down. Current anti-virus data files were updated and all accounts were scrubbed. Users were given instructions on how to install current anti-virus files. Infected workstations were taken off-line.

What support did you receive from ACERT/RCERT/ANSOC? Was this support timely?

Received virus update files from ACERT/ANSOC, with user information. Service was very timely.

What support did you need but did not receive?

None

What are your recommendations on how future attacks should be handled?

Same way due to limited resources of all components. Early notification is the key.

What support can HQ FORSCOM provide that would help you in these situations?

Possibly early warning from MACOM EOC. Probably not feasible, but again early warning is the key because the DoD will always be a little behind the power-curve on new viruses. It is the nature of the beast. If we are reacting, then the logic is we are reacting to an event that is out of our control. There is no 100% cure-all answer to virus protection. All we can do is react quickly as possible to limit the damage. To add, this is not an issue that is endemic to the Army, it is endemic to all who use DoD infrastructure AIS and even to the civilian populous.

APPENDIX 7 (FORT LEWIS) TO ANNEX F (INSTALLATIONS" LESSONS LEARNED) TO "ILOVEYOU" VIRUS LESSONS LEARNED REPORT

FT LEWIS

AV Product	# Networks	# Computers	OS	Impact	Damage	Source	Lost	# Files	Estimated
	Infected	Infected					Manhours	Infected	Costs - $
Norton	1	89	Win95,98,NT	Partial	Rebuild	Email	1100	Unk	6800

When and how did you first find out about the virus?

Fort Lewis found out about the virus via JTF-CND (SIPRNET). At approximately 06:30 hrs PDT the Systems Division Chief discovered the "ILOVEYOU" virus alert posted on CND web-site while performing routine (start of day) systems check.

What actions did you take and what were the results?

Based on the JTF-CND Alert, an immediate check of the Exchange email system revealed that Fort Lewis indeed, was already receiving infected mail messages (mostly from FORSCOM HQ sources). Briefed the Commander, 1115th Signal Battalion and shutdown SMTP Gateways, MTA, and Message Stores. Shutdown was completed by 07:15 hours. While awaiting an updated signature list an emergency meeting was held with unit IMO personnel. During this meeting DOIM disseminated information and provided instruction concerning the recovery of Exchange and the scanning of Personal Computers. After the signature list update was posted (on the RCERT website) the DOIM downloaded, updated local lists and initiated manual scanning of Exchange while IMO/SA's did the same with PC's and servers. After Exchange manual scanning was completed service was restored with a 7kb size restriction at the SMTP Gateways. This restriction was removed 24-hours later.

What support did you receive from ACERT/RCERT/ANSOC? Was this support timely?

DoD Cert provided a timely posting signature lists and the repair "fix". RCERT provided a web-page specific to the "ILOVEYOU" virus. This was easy to use and intuitive (didn't have to think through all the product offerings). ACERT provided expert advise (reformat the drive, was probably the smartest advise). No one site could be classified as all inclusive...and connection to vendor sites (Symantec & McAfee) were nearly impossible.

What support did you need but did not receive?

(6d) Fort Lewis did not receive a timely alert. It would have seemed that CERT's would have alerted sister CERT's,,, and it would have seemed that CERT's would have alerted supported Installations (telephonically). Fort Lewis had previously provided 24-hour points of contact (the 1115th Signal Battalion Message Center and/or Fort Lewis Staff Duty Officer).

What are your recommendations on how future attacks should be handled?

Alert notification needs improvement. A widespread and active attack within the DoD network ought to be treated as a 24 hour emergency (might establish criteria for severity i.e. emergency, urgent, routine). Need positive control alerting procedures (telephonic, email, web) depending upon severity. Might consider INFO alerts as having an Installation Staff Duty function i.e. use "Green Phone" to scramble DOIM personnel and alert units as to the situation.

OTHER LESSONS:

During peak periods of traffic, peak virus loads, etc Norton For Exchange may not keep up with the load. SA personnel witnessed Exchange delivering the infected messages, with Norton "lagging behind" seconds, up to many minutes later to "clean" the message. During this period users can (and did) open the infected message, triggering further infection. If the user's mailbox is configured to deliver to a personal mailbox (on the Personal Computer), Norton For Exchange may not "clean" the message (ever).

Secondary infection via commercial ISP email services (HotMail, Yahoo, etc) may present a "backdoor" threat.

Setting of INFOCON was helpful in providing checklist things to do and in disseminating the seriousness of this alert locally. Recommend such practice be continued.

IAVA alert procedures were helpful in disseminating information and gathering dataCall information. Need a tool to help streamline the process of gathering information from 137 reporting units.

Daily status reports seemed helpful in communicating status and problems to FORSCOM...need a method of sharing status, problems, pitfalls, workarounds and solutions amongst Installations.

Found Elron Internet Manager helpful in detecting which computers (by IP address) had accessed the SKYINET.NET web site i.e. to identify those who had potentially compromised user-id and password information.

-Rich Baasch-
C., Systems
1115th Signal Battalion
Fort Lewis, WA

APPENDIX 8 (FORT MCPHERSON) TO ANNEX F (INSTALLATIONS" LESSONS LEARNED) TO "ILOVEYOU" VIRUS LESSONS LEARNED REPORT

FT MCPHERSON

AV Product	# Networks	# Computers	OS	Impact	Damage	Source	Lost	# Files	Estimated
	Infected	Infected					Manhours	Infected	Costs - $
Norton	3	925	Win95,98,NT	Recovered	Rebuild	Email	1400	4050	7000

Question: When and how did you find out about the virus? Our Headquarters noticed a suspect email attachment from an unfamiliar sender as of 0645 on Thursday, 4 May 00 when a FORSNET helpdesk employee checked his email and he deleted the suspect message from his inbox. Fifteen minutes later, the helpdesk received a call that a user opened a similar attachment and his email was generating a tremendous volume of outgoing mail. This user was instructed to shutdown his system and disconnect it from the unclassified network. The S&N Division suspected a virus attachment that the current Norton Anti Virus (NAV) .dat file did not quarantine or eliminate. By about 0715, 3rd Army was also in the process of shutting down the post email servers due to the extent of the virus impact. For those users who had not yet opened their email, they were told to delete the messages. Those users who attempted to log in after 0740, found that the LAN would be unavailable for the rest of the day.

Question: What actions did you take and what were the results?
The S&N Division directed an SA to evaluate the first PC's symptoms and simultaneously contact the RCERT and Symantec to determine if the virus is a precursor to a massive virus attack. At 0730 on 4 May 00, the Chief, S&N Division decided to place all mail servers off-line immediately to prevent further infection. Next, to notify all FORSNET users of the virus attack with a brief explanation of its characteristics and not to open the suspect email and call a S&N Crisis Action team meeting to discuss the best responsive and repair actions.

Users at all levels were immediately informed of the virus. All infected computers were identified and physically disconnected from the network until further guidance was received from FORSNET.

At 0800 the S&N Division obtained adequate information from RCERT and the vendor regarding the characteristics of the virus and a temporary fix patch designed to capture and quarantine the virus upon scanning of the mail servers. The Chief, S&N Division implemented the emergency recovery procedures that included the mail servers in off-line status to prevent further damage to the Army networks while network scanning was initiated. FORSNET was without email services for approximately 22 hours from 0800, 4 May through 0600, 5 May 2000.

During the email downtime, several measures were taken to prevent the spread of the virus from within the headquarters and to guard against receiving additional messages containing the virus from outside FORSNET. The S&N Division implemented the updated virus definition files developed by Symantec and approved by ACERT and forced users to logoff/on to protect the non-infected workstations and servers.

Question: What support did you receive from ACERT/RCERT/ANSOC? They provided reactive guidance on what needed to be accomplished with infected systems. We obtained information on the virus from ACERT and Assist Web sites and Norton's web site on the Internet.
SUBJECT: Lessons Learned After Action Report for the ILOVEYOU Worm Virus

Was this support timely? Yes

What are your recommendations on how future attacks should be handled? The FORSNET must develop a quick reaction checklist to effectively manage significant network operational crisis and to provide initial crisis notification to management. The checklist will greatly improve notification for both internal and external to the FORSNET users and promptly exchange the necessary information. Upon infection by the ILY virus, the CRC member was assembled on the fly. Though the cell quickly assembled and was composed of the correct experts and leaders, there is still a need for improvement. Once assembled, the cell maintained positive command and control over the situation and provided timely information and recommendations to the leadership. The CRC requires a dedicated space to manage the crisis, which provides sufficient voice and data communications from the beginning to the end of the crisis. FORSNET must possess a dynamic inbound email scan tool that can be set to scan for specific file types and/or word/phrases. Currently, the S&N Division is evaluating software.

f. What support can HQ, FORSCOM provide that would help you in these situations?
FORSCOM IAO provided the INFOCON posture and procedural information support during this virus attack. Recommend notification to changes in FORSCOM INFOCON posture continue to be disseminated through its DCSC4 web site, normal message traffic, and/or via telephone calls.

POC this memorandum is Mr. Lou Fusco, Chief of S&N Division, DCSC4,(DSN) 367-6796.

/Original signed/

APPENDIX 9 (FORT POLK) TO ANNEX F (INSTALLATIONS" LESSONS LEARNED) TO "ILOVEYOU" VIRUS LESSONS LEARNED REPORT

FT POLK

AV Product	# Networks	# Computers	OS	Impact	Damage	Source	Lost	# Files	Estimated
	Infected	Infected					Manhours	Infected	Costs - $
Norton/McAfee	1	70	Win95,98,NT	Partial	Rebuild	Email	1,300	Unk	2100

When and how did you first find out about the virus?

Between the hours of 0715-0745 CDT 4 May 2000 by various means--User experience, News Reports, and Phonecon from ACERT.

What actions did you take and what were the results?

Shut down primary email servers until AV update was available. This prevented in excess of 15,000 copies of infected email being delivered to users. Formed an emergency working group composed of all available SA's and NA's with ISSO support and used all means available to identify systems that may have been infected.

What support did you receive from ACERT/RCERT/ANSOC? Was this support timely?

Early warning by telephone from ACERT was an important event. Otherwise, we may have wasted precious time in determining seriousness of event. Received good telephonic support from ACERT and RCERT during event, especially considering the number of calls they were probably getting.

What support did you need but did not receive?

We are of the opinion that extent of probable damage assessement by the ACERT took too long, and that requirements to clean systems were probably overkill. More local assessment should be allowed, assuming that the technical expertise exists, and good risk analysis procedures are used.

What are your recommendations on how future attacks should be handled?

Refine the process to use all communications capability to get the message out. This incident showed the vulnerability of email, which is the primary notification medium. While telephone and fax were used in this incident, there were conflicts in specific detail about requirements, especially in the INFOCON implementation.

What support can HQ FORSCOM provide that would help you in these situations?

Fund a planning and training session or sessions for the Headquarters and FORSCOM installations with the focus on FORSCOM mission, needs and procedures.

APPENDIX 9 (FORT POLK) TO ANNEX F (INSTALLATIONS" LESSONS LEARNED) TO "ILOVEYOU" VIRUS LESSONS LEARNED REPORT

Although lessons learned with only local impact was not a requirement for this report, we found that we need a better notification and tasking system within the installation. We experienced a good bit of confusion, especially early on. If the event had occured on a weekend or holiday, the negative results could have been much more substantial. We are working on a fix within the ISS Working Group.

APPENDIX 10 (FORT RILEY) TO ANNEX F (INSTALLATIONS" LESSONS LEARNED) TO "ILOVEYOU" VIRUS LESSONS LEARNED REPORT

FT RILEY

AV Product	# Networks	# Computers	OS	Impact	Damage	Source	Lost	# Files	Estimated
	Infected	Infected					Manhours	Infected	Costs - $
Norton	1	280	Win95,98, NT	Unk	Rebuild	Email	1135	115,332	4000

Question 6A. When and how did you find out about the Virus?

Answer: The Virus was discovered on 4 May 00 approximately 0630 by a soldier in building 200, who opened the "I Love You" attachment and informed G6/DOIM on Ft. Riley of what happened to his computer.

Question 6B. What actions did you take and what were the results?

Answer: (1) The computer was disconnected from the LAN by the soldier
(2) Alert call in procedures was initiated
(3) Advised server personnel to shut down e-mail
(4) Notified all concerned sections of virus
(5) Scheduled meeting for update on virus
(6) Initiated proper procedures to quarantine and fix the virus to include updating
(7) Coordinated with ACERT and requested knowledge shared with FORSCOM and other installations concerning actions taken on a fix for the virus
(8) Sent MSG's through installation FROC notifying all commanders, agencies and IMO's to update latest antivirus via the intranet. Also notifying all agencies not to open the "I Love You" virus, and to delete the 20 different subject lines.
(9) Updated servers
(10) Continued coordination with FORSCOM, ACERT, and other installations
(11) INFOCON implemented
(12) Testing "Antigen" AV software along with Norton as primary
(13) Found Antigen to be more user-station friendly
(14) Notified FORSCOM of ANTIGEN findings
(15) Running antigen AV on e-mail notified FORSCOM general on ANTIGEN AV software

Question 6C. What support did you receive from ACERT/RCERT/ANSOC? Was this support timely?

Answer: (1) Reporting of virus damage assessment
(2) No

Question 6D. What support did you need but did not receive?
Answer: N/A

Question 6E. What are your recommendations on how future attacks should be handled?
Answer: Adhere to local Standard Operating Procedures (SOP)/Security policies which are in place

Question 6F. What support can HQFORSCOM provide that would help you in these situations?
Answer: (1) Funding for AV Software
(2) alleviate constant reporting procedures to higher headquarters

APPENDIX 11 (FORT STEWART) TO ANNEX F (INSTALLATIONS" LESSONS LEARNED) TO "ILOVEYOU" VIRUS LESSONS LEARNED REPORT

FT STEWART

AV Product	# Networks	# Computers	OS	Impact	Damage	Source	Lost	# Files	Estimated
	Infected	Infected					Manhours	Infected	Costs - $
Norton/McAfee	1	120	Win95,98,NT	Unk	Rebuild	Email	650	Unk	11700

6A. WHEN AND HOW DID YOU FIND OUT ABOUT THE VIRUS? When it was reported on-site.

6B. WHAT ACTIONS DID YOU TAKE AND WHAT WERE THE RESULTS. Disconnected until a fix/quarantine was in place. Notified all users through EOC channels, disconnected systems infected, Blocked IP systems were attempting to transmit to, Provided information to users as soon as it was available.

6C. WHAT SUPPORT DID YOU RECEIVE FROM ACERT/RCERT/ANSOC? WAS THIS SUPPORT TIMELY? As much as they could, but they were as dependent on the anti-virus vendors to provide a fix/quarantine as we were. They provided needed information through their web site and provided a fix as soon as it was available.

6D. WHAT SUPPORT DID YOU NEED BUT DID NOT RECEIVE? None

6E. WHAT ARE YOUR RECOMMENDATIONS ON HOW FUTURE ATTACKS SHOULD BE HANDLED? The DOIM is establishing a program to automatically update the anti-virus product when a network user logs onto the domain. We cannot protect systems when there is no product available, but we can ensure all users have the most current update through automation.

6F. WHAT SUPPORT CAN HQFORSCOM PROVIDE THAT WOULD HELP YOU IN THESE SITUATIONS? If FORSCOM or any other organization has a method of "automatically updating" the anti-virus product through the network it would be beneficial to this Installation. One problem is the fact we have multiple operating systems on the Ft Stewart domain, i.e., Windows NT, Windows 95/98, Unix, Novell, and upgrading/migrating to Windows 2000.

APPENDIX 12 (FORT 32D AAMDC) TO ANNEX F (INSTALLATIONS" LESSONS LEARNED) TO "ILOVEYOU" VIRUS LESSONS LEARNED REPORT

32d AAMDC

Question: When and how did you find out about the virus? Our Headquarters and subordinate ADA Brigades found out about the virus as early as 0500 hours on Friday, 28 Apr 00 when users were checking their email during normal operations. Users noticing the ILOVEYOU virus reported the messages in their inbox to their respective Information Management Officers and to the Fort Bliss DOIM. They were instructed to disconnect their system from the unclass LAN. The G6 was CC'd of their situation. By about 0715 hours, the DOIM was also in the process of shutting down the post email servers due to the extent of the virus' impact. For those users who had not yet opened the email, they were told to delete the messages. Those users who attempted to log in after 0730 hours found out the LAN would not be available for the rest of the day.

Question: What actions did you take and what were the results? Users at all levels were immediately informed of the virus. In the first 24 hours, computers that were infected were identified and physically disconnected from the network until further guidance was received from post. FORSCOM INFOCON procedures for INFOCON ALFA and BRAVO were reviewed and appropriate actions were taken IAW FORSCOM INFOCON BRAVO. (Note that the TRADOC side of Ft Bliss was in normal status while FORSCOM units were at INFOCON BRAVO). Unit reaction teams were dispatched to ensure users had the most recent anti-virus/signature update and knew what steps to take if the virus was emailed to them. The patches were installed on the Brigades' servers and on machines coming directly off the post DOIM server. Infected systems were cleaned ICW guidance from FORSCOM Information Assurance office and the Fort Bliss DOIM.

Question: What support did you receive from ACERT/RCERT/ANSOC? They provided reactive guidance on what needed to be accomplished with infected systems. Our IMOs obtained information on the virus from ACERT and Assist Web sites and the Norton's web site on the internet.

Was this support timely? Yes

What are your recommendations on how future attacks should be handled?
The FORSCOM units at Ft Bliss did not know the Information Assurance (IA) office was standing up a Crisis Action Team (CAT) at the FORSCOM level to respond to this situation until one day after it was established. When a FORSCOM CAT team is about to be stood up, recommend the IA notify the post DOIM (via post EOC after duty hours), and treat as a Commander's Critical Information Requirement (CCIR), even though the latter agency falls under TRADOC. The local DOIM can then disseminate relevant information to unit FORSCOM IMOs on post, including the 32d AAMDC, in much the same manner

that Y2K transition rollover was handled. Notifying FORSCOM users via communications center message traffic with appropriate level precedence should be continued. Because TRADOC units were in normal status while FORSCOM units were in INFOCON BRAVO, FORSCOM units will adhere to the more stringent posture as required. 32d AAMDC will deconflict appropriate measures for units under its C2, in close coordination with the local DOIM.

What support can HQ, FORSCOM provide that would help you in these situations?

FORSCOM IA provided rock solid support during this virus attack. Recommend notification to changes in FORSCOM INFOCON posture continue to be disseminated through its DCSC4 web site, normal message traffic, and/or via telephonic means.

POC this memorandum is the undersigned, DSN: 978-7597.

/Original signed/
REYNOLD F. PALAGANAS
LTC, SC
Assistant Chief of Staff, G6

APPENDIX 13 (JTF-6) TO ANNEX F (INSTALLATIONS" LESSONS LEARNED)
TO "ILOVEYOU" VIRUS LESSONS LEARNED REPORT

JTF-6

Eleven people in JTF-6 opened the "ILOVEYOU" virus onThursday, 4 May. We have no excuse as this was an item of instruction during the "Melissa" virus alert. We shut down those eleven machines, isolated ourselves from the Internet and shut down e-mail. We also locked out all remote users until it could be verified that their machines were clean. We were isolated for about twelve hours. Throughout this process we operated without guidance. Only one remote user opened the virus-infected attachment. He is still locked out until he returns from TDY and we can wipe the drives and reprogram. We confined and destroyed the virus, cleaned all the servers, all mail accounts and all drives ensuring no .vbs (file extension) attachment remained. Affected machines were wiped clean and reprogrammed. Deliberate action (not UCMJ - may come to that later) was taken against those who failure to follow our instructions which resulted in our sytem being infected. Our system is operating smoothly, however, not sure of any residual effects.

Anderson, Dorian

ANNEX G (FORSCOM INFOCON MESSAGES) TO “ILOVEYOU” VIRUS LESSONS LEARNED REPORT

FORSCOM INFOCON MESSAGES

APPENDIX 1 (DOWNGRADE TO ALPHA) TO ANNEX G (FORSCOM INFOCON MESSAGES) TO "ILOVEYOU" VIRUS LESSONS LEARNED REPORT

```
RAAUZYUW RUEASRB0005 1371826-UUUU--.
ZNR UUUUU
R 171826Z MAY 00
FM CDRFORSCOM FT MCPHERSON GA//AFCI-JI//
TO AIG 2028
AIG 7479
INFO USCINCJFCOM NORFOLK VA//J3/J6//
DA WASHINGTON DC//DAMO-ODZ/SAIS-ZA//
BT
UNCLAS
MSGID/GENADMIN/CDR FORSCOM AFCI-JI//
SUBJ/FORSCOM DOWNGRADE TO INFOCON ALPHA//
REF/A/MSG /HQ FORSCOM /041545Z//
REF/B/MSG /HQ FORSCOM/060053Z//
NARR/REF A:  SUBJECT:  FORCES COMMAND INFORMATION OPERATIONS
CONDITION (INFOCON) CHANGE TO BRAVO.
REF B:  SUBJECT:  CLARIFICATION OF FORSCOM DECLARATION OF INFOCON
BRAVO.  //
POC/NATE PERKINS/LTC/FORSCOM/LOC:FORT MCPHERSON, GA/TEL:DSN 367-7515
//
POC/DON LABONTE/MR./FORSCOM/LOC:FORT MCPHERSON, GA/TEL:DSN 367-6467//
POC/TOM BLACKBURN/MR./FORSCOM/LOC:FT MCPHERSON/TEL:DSN 367-5023//
RMKS/1.  FORSCOM HAS DOWNGRADED INFOCON TO ALPHA.
2.  VARIANTS OF THE ILOVEYOU WORM VIRUS CONTINUE TO BE A THREAT AND
ALL ACTIVITIES SHOULD CONTINUE TO WORK NETWORK DEFENSE AND RECOVERY
MEASURES.
3.  WORKSTATIONS THAT HAVE BEEN INFECTED MAY NOT BE PLACED BACK
ONLINE UNTIL THE ISSO CERTIFIES THAT THEY ARE CLEAN.
4.  THE FOLLOWING INFOCON ALPHA MEASURES APPLY:
4A.  MEASURE A-3. ENSURE THAT ALL USERS, SYSTEMS ADMINISTRATORS AND
SYSTEM SECURITY PERSONNEL ARE AWARE OF THE THREAT AND RESPONSE
MEASURES.
4B.  MEASURE A-4.  REMIND ALL USERS TO SCAN FLOPPY DISKS BEFORE USE.
4C.  MEASURE A-8.  ENSURE THAT PASSWORD MANAGEMENT PROGRAM COMPLIES
WITH AR 380-19.
4D.  MEASURE A-10.  ENSURE THAT SYSTEM AND NEWORK SYSTEM
ADMINISTRATORS HAVE A CURRENT LIST OF BLOCKED IP ADDRESSES.
4E.  MEASURE A-12.  ENSURE THAT THE MOST CURRENT ANTIVIRUS DAT FILES
ARE DOWNLOADED AND IMPLEMENTED
5.  UNTIL FURTHER NOTICE, PROVIDE DAILY SITREP NLT 1400 EDT  TO HQ
FORSCOM DCSC4 THROUGH INFORMATION ASSURANCE CHANNELS.
6.  REQUEST A LESSONS LEARNED REPORT NLT 2 JUN 00 ADDRESSING THE
FOLLOWING:
6A. WHEN AND HOW DID YOU FIND OUT ABOUT THE VIRUS?
6B. WHAT ACTIONS DID YOU TAKE AND WHAT WERE THE RESULTS.
6C. WHAT SUPPORT DID YOU RECEIVE FROM ACERT/RCERT/ANSOC?  WAS THIS
SUPPORT TIMELY?
6D. WHAT SUPPORT DID YOU NEED BUT DID NOT RECEIVE?
6E. WHAT ARE YOUR RECOMMENDATIONS ON HOW FUTURE ATTACKS SHOULD BE
HANDLED?
6F. WHAT SUPPORT CAN HQFORSCOM PROVIDE THAT WOULD HELP YOU IN THESE
SITUATIONS?
6.  FORSCOM POCS:  LTC NATE PERKINS (DSN 367-7515), DON LABONTE (DSN
367-6467), TOM BLACKBURN (DSN 367-5023).//
BT
#0005
```

APPENDIX 2 (CLARIFICATION OF BRAVO) TO ANNEX G (FORSCOM INFOCON MESSAGES) TO "ILOVEYOU" VIRUS LESSONS LEARNED REPORT

OTTUZYUW RUEASRB0872 1260053-UUUU--RUERAIX RUEREUX RUERGAA
RUERGAB
RUERGAJ RUERGAM RUERGAR RUERLEX RUERNUA RUERNUB RUERNUK
RUERNUL
RUERNUS RUERUCX.
ZNR UUUUU
O 060053Z MAY 00
FM CDRFORSCOM FT MCPHERSON GA//AFOP-CAT//
TO /AIG 2028//
INFO AIG 7479//
BT
UNCLAS
MSGID/GENADMIN/FORSCOM AFOP-CAT//
SUBJ/CLARIFICATION OF FORSCOM DECLARATION OF INFOCON BRAVO//
REF/A/MSG/HQFORSCOM/041545ZMAY00//
NARR/REF A IS FORSCOM MESSAGE DIRECTING CHANGE OF INFOCON FROM NORMAL TO BRAVO//
POC/PERKINS/LTC/DCSC4, HQ FORSCOM/TEL:DSN 367-7515//
AKNLDG/NO//RMKS/

1. REF MESSAGE 041545Z MAY 00, AFOP-CAT, SUBJECT: FORCES COMMAND INFORMATION OPERATIONS CONDITION (INFOCON) CHANGE TO BRAVO.

2. ELEVATION OF INFOCON TO BRAVO IS BASED ON THE IMPACT THAT COMPUTER VIRUS (ILOVEYOU) HAS HAD ON ARMY EMAIL SYSTEMS. THIS IS A WORM VIRUS WHICH RAPIDLY REPLICATES ITSELF THROUGHOUT THE NETWORK BY SENDING COPIES OF ITSELF TO ALL ADRESSEES IN A USERS ADDRESS BOOK WHEN THE ATTACHED FILE IS OPENED. IN ADDITION, THE WORM CORRUPTS OR DESTROYS SPECIFIC FILES ON THE USERS HARD DRIVE AND COMPROMISES PASSWORDS.

3. SINCE THE INITIAL WORM ATTACK, THERE HAVE BEEN VARIANTS WHICH HAVE A DIFFERENT NAME IN THE SUBJECT LINE OF THE EMAIL MESSAGE SO THE ATTACK CANNOT BE DETECTED BASED ON SUBJECT LINE ALONE. THE COMMON DENOMINATOR FOR ALL VERSIONS OF THIS VIRUS APPEARS TO BE THE ATTACHMENT WITH (VBS) IN THE EXTENSION.

4. DIRECTED INFOCON ALPHA AND BRAVO MEASURES CLARIFICATION:

4A INFOCON ALPHA.

4A(1). MEASURE A3: ENSURE ALL SECURITY MANAGERS, INFORMATION SYSTEM SECURITY MANAGERS (ISSM), INFORMATION SYSTEM SECURITY OFFICERS (ISSO), SYSTEM ADMINISTRATORS (SA), COMSEC CUSTODIANS, AND OTHER COMMUNICATIONS OR INFORMATION SYSTEMSORGANIZATIONS ARE INFORMED OF THE IO THREAT ACTIVITY AND RESPONSE MEASURES.

4A(2). MEASURE A-6: REMIND ALL USERS THAT SCANNING COMPUTER FLOPPY DISKS FOR VIRUSES IS MANDATORY PRIOR TO USE.

4A(3). MEASURE A-7: REMIND ALL USERS TO REPORT UNUSUAL ACTIVITY, VIRUSES, AND POTENTIAL DENIALS OF SERVICE OF COMPUTER, SATELLITE, OR TELEPHONE SYSTEMS (INCLUDING FAX MACHINES). REPORT UNUSUAL

ACTIVITY IN ACCORDANCE WITH ESTABLISHED ARMY AND LOCAL INCIDENT REPORTING PROCEDURES.
4A(4). MEASURE A-9: ENSURE THAT REQUIREMENTS OF NETWORK SECURITY IMPROVEMENT PROGRAM (NSIP) AND INFORMATION ASSURANCE VULNERABILITY ALERT (IAVA) DIRECTIVES HAVE BEEN MET OR ARE BEING WORKED.
4A(5). MEASURE A-10: UPDATE AND DISTRIBUTE LIST OF INTRUDER INTERNET PROTOCOL (IP) ADDRESSES FOR LOCAL IP HOT-LISTS TO SAS.
4A(6). MEASURE A-11: UPDATE INDICATIONS AND WARNING ATTACK SIGNATURES, PROFILES, AND METHODS OF RECENT ATTACK FOR USE BY INTRUSION DETECTION SYSTEMS, AND FOR USE BY SA TO MANUALLY DETECT INTRUSIONS. ALARM LEVELS OF AUTOMATED INTRUSION DETECTION SYSTEMS SHOULD BE ADJUSTED TO PROVIDE APPROPRIATE ALERT THRESHOLDS.
4A(7). MEASURE A-12: SA WILL UPDATE ALL VIRUS SOFTWARE AND DAT FILES ON SERVERS AND DIRECT USERS TO DO SO ALSO IF APPLICABLE. ALL WORKSTATIONS WILL BE SCANNED FOR VIRUSES.4A(8). MEASURE A-14: SA WILL ENSURE ROUTERS AND FIREWALLS PROTECTING ALL SEGMENTED CRITICAL C4I NETWORKS HAVE PROPER CONFIGURATION SETTINGS TO GUARD AGAINST KNOWN VULNERABILITIES AND METHODS OF RECENT ATTACKS.
4A(9). MEASURE A-17: ENSURE THAT THERE ARE LOCAL PROCEDURES TO ASSESS AND IMPLEMENT THE DIRECTIVES STATED IN THE INFOCON MESSAGE IN THE TIMEFRAME REQUIRED. THIS INCLUDES PROCEDURES TO CONTACT KEY INFORMATION ASSURANCE PERSONNEL AFTER DUTY HOURS.
5A. INFOCON BRAVO.
5A(1). MEASURE B-2: DIRECT ALL ISSM, ISSO, AND SA TO INCREASE SECURITY AWARENESS, PARTICULARLY FOR CRITICAL C4I SYSTEMS, AND PLACE THEM ON ALERT FOR POSSIBLE RECALL AFTER NORMAL DUTY HOURS.
5A(2). MEASURE B-3: CLOSE ALL REMOTE MAINTENANCE PORTS ON VULNERABLE OR AFFECTED ROUTERS, FIREWALLS, SERVERS, COMPUTER-BASEDTELEPHONE SWITCHES, AND ANY OTHER ACCESSIBLE INFORMATION SYSTEMS.
5A(3). MEASURE B-4: SA WILL REDUCE DIAL-IN ACCESS ON CRITICAL C4I SYSTEMS TO MINIMUM ESSENTIAL PERSONNEL AS DIRECTED BY DCSOPS,G3.
5A(4). MEASURE B-5: NOTIFY POST,BASE,CAMP LAW ENFORCEMENT AND EMERGENCY PERSONNEL OF INFOCON STATUS.
5A(5). MEASURE B-6: SA WILL REVIEW NETWORK MONITORING LOGS, SYSTEM AUDIT LOGS, AND SERVER SYSTEM LOG FILES FOR EVIDENCE OF SPECIFIED UNUSUAL OR MALICIOUS ACTIVITY.
6. NEW MEASURE: WARN ALL USERS NOT TO OPEN EMAIL WITH ILOVEYOU IN THE SUBJECT LINE AND TO DELETE IT AND NOT TO OPEN ANY EMAIL ATTACHMENT THAT HAS (VBS)IN THE EXTENSION.
7. NEW MEASURE: IF ATTACHMENT HAS BEEN OPENED, THE USER MUST SHUT DOWN THE WORKSTATION AND CONTACT THE APPROPRIATE ISSO. THE WORKSTATION MUST BE PURGED OF THE VIRUS, MODIFIED FILES DELETED

AND THE PASSWORD CHANGED BEFORE REGAINING ACCESS TO THE NETWORK.

8. ACERT HAS ISSUED IAVA A2000-0007 VBS.LOVELETTER THREAT. SINCE SA MAY NOT HAVE RECEIVED THIS NOTICE VIA THE ACERT LISTSERVER DUE TO EMAIL DEGRADATION, THEY SHOULD GO TO THE ACERT WEBSITE, HTTP(SLASH)(SLASH)WWW.ACERT.BELVOIR.ARMY.MIL(SLASH)FRAMES.HTML, TO OBTAIN THE LATEST INFORMATION REGARDING THIS VIRUS THREAT.

9. IN CONJUNCTION WITH THE IAVA REPORTING REQUIREMENT, INSTALLATIONS ARE TO PROVIDE A DAILY REPORT OF STATUS OF EMAIL CAPABILITY NLT 0700 EDT. REPORT WILL BE SUBMITTED TO DON LABONTE, FAX 404-464-7201,DSN 367-7201. REPORT ELEMENTS ARE:

9A. MAIL SERVER STATUS: ONLINE-NO DEGRADATION,ONLINE-DEGRADATION, OFFLINE. IF OFFLINE, PROJECTED TIME EMAIL SERVICE WILL BE RESTORED.

9B. WORKSTATIONS INFECTED: (I.E. USERS WHO OPENED ATTACHMENT) ALSO SHOW AS PERCENTAGE OF TOTAL WORKSTATIONS ON NETWORK.

9C. ANTIVIRUS SOFTWARE STATUS: (I.E., HAVE THE MOST CURRENT DAT FILES BEEN DOWNLOADED AND IMPLEMENTED,DOWNLOADED BUT NOT IMPLEMENTED,NOT DOWNLOADED)

9D. RECOVERY PLAN: SUMMARIZE ACTIONS TAKEN TO DEAL WITH THIS THREAT. STATE IF ACTIONS ARE COMPLETE OR ONGOING

10. FORSCOM POCS: LTC NATE PERKINS (DSN 367-7515), DON LABONTE (367-6467), TOM BLACKBURN (DSN 367-5023). THE DCSC4 CRISIS ACTION TEAM TELEPHONE NUMBER IS COMMERCIAL: (404) 464-7989, DSN:367-7989 (STU-III).//

BT

APPENDIX 3 (DECLARE BRAVO) TO ANNEX G (FORSCOM INFOCON MESSAGES) TO “ILOVEYOU” VIRUS LESSONS LEARNED REPORT

```
OAAUZYUW RUEASRB0870 1251459-UUUU--RUEASRB RUERPHB
RUEASRT RUERGIA.
ZNR UUUUU
O 041545Z MAY 00
FM COMFORSCOM FT MCPHERSON GA//AFOP-CAT//
TO RUERSHA/CDRUSAFIVE AND FT SAM HOUSTON TX//AFKB-OP/GT/TR//
RUERGIA/CDRUSAONE FT GILLEM GA//AFKA-OP/TR//
RUEASRT/CDRUSATHIRD FT MCPHERSON GA//AFRD-OP//
RUERHNA/CDRXVIIIABNCORPS AND FT BRAGG NC//AFZA-GT/GT-EOC//
RUERBFA/CDRIIICORPS FT HOOD TX//AFZF-GC/GT/OP//
RUEAFDC/CDRICORPS FT LEWIS WA//AFZH-GC/GT/OP/PTM-OO//
RUEASRB/CDRUSARC FT MCPHERSON GA//AFRC-O/OP//
RUEASRB/CDR52DORDGPEOD FT GILLEM GA//AFYB-S3/S6//
RUERLEX/CDR49THQMGP FT LEE VA//AFFL-G//
RHMFIUU/CDR49THQMGP FT LEE VA//AFFL-G//
RUERSWA/CDR3DINFDIV MECH FT STEWART GA//AFZP-GC//
RUERFDA/CDR10THMTNDIV LI FT DRUM NY//AFZS-GC//
RUEAPFA/CDR101STABNDIV AASLT FT CAMPBELL KY//AFZB-GC//
RHMFIUU/CDR101STABNDIV AASLT FT CAMPBELL KY//AFZB-GC//
RUERNUB/CDRADARTYCEN FT BLISS TX//ATSA//
RUEACQC/CDR FT CARSON CO//AFZC-GC//
RUERUCX/CDR FT HUACHUCA AZ
RUERUCD/CDRUASC FT HUACHUCA AZ//AFSC-OP//
PAGE 02 RUEASRB0870 UNCLAS
RUEASRB/CDR FT MCPHERSON GA
RUEASRB/CDR FT GILLEM GA
RUERNKU/CDRFTRILEYKS//AFZN-GC//
RUERNUS/CDRUSAFAC FT SILL OK//ATZR-FO//
RUERDGA/CDRJRTC FT POLK LA//G3/CS/AFZX-GC/GT//
RHMFIUU/CDRJRTC FT POLK LA//G3/CS/AFZX-GC/GT//
RUEAFIF/CDRNTC FT IRWIN CA//AFZJ-GC/PT//
RUERBEN/CDRUSAISC FT BENNING GA//ATZB-DPT//
RUEREUX/CDRTRANSCEN FT EUSTIS VA//ATZF-GC/GD//
RUERLEX/CDRUSACASCOM FT LEE VA//ATZM-GC//
RUERNUS/CDR FT SILL OK//ATZR-P//
RUEABSA/CDR FT DIX NJ//AFRC-GC//
RUEADFA/CDR FT MCCOY WI//AFRC-CG//
RUERNUS/CDRIIICORPSARTY FT SILL OK//S3/S6//
RUEREUX/CDR7THTRANSGP FT EUSTIS VA//AFFG-C-PL//
RUERGAB/CDR36THENGRGPCBT FT BENNING GA//S3/S6//
RUEOEGA/CDRARCENT KUWAIT DOHA KU
RUERSWA/CDR3RDINDIVMECH FT STEWART GA//S3/S6//
RUERDGA/CDR2NDACR FT POLK LA//G3/G6//
RUEACQC/CDR3DACR FT CARSON CO//S3/S6//
```

```
PAGE 03 RUEASRB0870 UNCLAS
RUERNUB/CDR32NDAAMDC FT BLISS TX//AFVL-CG//
RUERGAA/CDR93RDSIGBDE FT GORDON GA//AFSA-O//
RUERUCX/CDRUSASC FT HUACHUCA AZ//AFSC-OPC-E//
RHMFIUU/CDRUSASC FT HUACHUCA AZ//AFSC-OPC-E//
RUERNUA/CDRUSAEC FT LEONARD WOOD MO
RUERGAB/CDRUSAIC FT BENNING GA// ATZB-LOP-P/ATSH-OTP//
RUSTRUK/CDRUSARAVN CENTER FT RUCKER AL
RUERUCX/CDRASC FT HUACHUCA AZ//ASOP-OM//
INFO RUCBACM/USCINCJFCOM NORFOLK VA//J52/J3/J33/J35/J7//
RUEKJCS/JOINT STAFF WASHINGTON DC//J3/J33-O/J322/J-3JOD/J4//
RUEADWD/DA WASHINGTON DC//DAMO-OD/O/M/SAIS/SAILE/SSP/
SAFM-VUO-C//
RUERAIX/CDRTRADOC FT MONROE VA//ATSC-EOC/ATTG-ZA/U/SE/ATPL//
RHCUAAA/USCINCTRANS SCOTT AFB IL//TCJ3/TCJ4/TCJ5-WD/TCJ5-SR//
RUEARNG/ARNGRC ARLINGTON VA//NGB-ARO-RM OC/R/ARL-LP/NGB-PA//
RUEAMDW/CDRMDW WASHINGTON DC
RUVAFMC/AFMC WRIGHT PATTERSON AFB OH//CV//
RHCUMAC/HQ AMC TACC COMMAND CENTER SCOTT AFB IL/XO/P//
RUEAAMC/CDRAMC ALEXANDRIA VA//AMCCB//
RUEADWD/DIRMILSPT ODCSOPS WASHINGTON DC//DAMO-ODS//
RHCUAAA/USCINCTRANS SCOTT AFB IL//TCJ3//
PAGE 04 RUEASRB0870 UNCLAS
RUEAMTC/CDRMTMC FALLS CHURCH VA //MTOP-O//
RUEREUX/CDRMTMCDSC FT EUSTIS VA  //MTDC-OPS//
RUERNLX/CDR 1108 SIG BDE FT DETRICK MD//AFSY-CDR//
RUERGFA/CDR 55 SIGNAL CO FT MEADE MD//AFSY-SRD//
RUEASRB/AFNSEP FT MCPHERSON GA//EP//
RUEASRB/COMFORSCOM FT MCPHERSON GA//AFOP//
BT
UNCLAS
OPER/INFOCON//
MSGID/GENADMIN/FORSCOM/DCSOPS//
SUBJ/FORCES COMMAND INFORMATION OPERATIONS CONDITION
(INFOCON) CHANGE TO BRAVO//
POC/LABONTE/DCSC4/FORSCOM/-/TEL:DSN 367-6467/TEL:COMM (404)
464-6467
//
RMKS/1.  ALL FORSCOM COMMANDS, INSTALLATIONS AND ACTIVITIES
WILL GO IMMEDIATELY TO INFOCON BRAVO.  LOCAL COMMANDERS
HAVE THE PEROGATIVE TO ESTABLISH A HIGHER INFOCON LEVEL WHEN
CONDITIONS WARRANT AND LEVEL IS APPROVED BY FORSCOM
DCSOPS.
```

2. MEASURES ASSOCIATED WITH INFOCON ALPHA AND BRAVO INCLUDE:

2A. INFOCON ALPHA.

PAGE 05 RUEASRB0870 UNCLAS

2A(1). MEASURE A-1: DISTIBUTE MESSAGE THROUGH COMMAND CHANNELS (DCSOPS) TO ALERT COMMANDERS OF THE INFORCON. MACOM WHICH OWN FACILITIES HOSTING FORSCOM UNITS/ACTIVITIES WILL BE INFO ADDRESSEES.

2A(2). MEASURE A-2: NOTIFY FORSCOM INSTALLATION C2P/IA POCS AND ANSOC OF INFOCON AND REQUIRED ACTIONS.

2A(3). MEASURE A-3: ENSURE ALL SECURITY MANAGERS, INFORMATION SYSTEM SECURITY MANAGERS (ISSM), SYSTEM ADMINISTRATORS (SA), COMSEC CUSTODIANS AND OTHER COMMUNICATIONS OR INFORMATION SYSTEMS ORGANIZATIONS ARE INFORMED OF THE THREAT IO ACTIVITY AND RESPONSE MEASURES.

2A(4). MEASURE A-4: ISSUE AN EMAIL TO REMIND ALL PERSONNEL TO INCREASE OPSEC AWARENESS. INCLUDE THINGS SUCH AS REMINDING ALL USERS OF THE RISKS OF BEING MONITORED BY ADVERSARIES DURING EMAIL AND PHONE USE.

2A(5). MEASURE A-5: REMIND ALL USERS TO IMMEDIATELY REPORT ANYONE REQUESTING DIRECT ACCESS OR COMPUTER PASSWORDS TO ACCESS C4I NETWORKS AND WORKSTATIONS.

2A(6). MEASURE A-6: REMIND ALL USERS THAT SCANNING COMPUTER FLOPPY DISKS FOR VIRUSES IS MANDATORY PRIOR TO USE.

2A(7). MEASURE A-7: REMIND ALL USERS TO REPORT UNUSUAL ACTIVITY,

PAGE 06 RUEASRB0870 UNCLAS

VIRUSES, AND POTENTIAL DENIALS OF SERVICE OF COMPUTER, RADIOTELEPHONE, SATELLITE, OR TELEPHONE SYSTEMS (INCLUDING FAX MACHINES). REPORT UNUSUAL ACTIVITY IN ACCORDANCE WITH ESTABLISHED ARMY AND LOCAL INCIDENT REPORTING PROCEDURES.

2A(8). MEASURE A-8: SA REQUIRE ALL COMPUTER SYSTEMS USERS TO CHANGE PASSWORDS WITHIN 48 HOURS. PASSWORDS WILL BE CHANGED EVERY 90 DAYS WHILE IN INFOCON ALPHA. ISSM, ISSO, AND SA WILL REMIND USERS OF THE NEED FOR PASSWORDS WITH A MINIMUM OF 8 RANDOM ALPHANUMERIC CAHRACTERS TO INCLUDE AT LEAST TWO NUMERICS.

2A(9). MEASURE A-9: ENSURE THAT REQUIREMENTS OF NETWORK SECURITY IMPROVEMENT PROGRAM (NSIP) AND INFORMATION ASSURANCE VULNERABILITY ALERT (IAVA) DIRECTIVES HAVE BEEN MET OR ARE BEING WORKED. 2A(10). MEASURE A-10: UPDATE AND DISTRIBUTE LIST OF INTRUDER INTERNET PROTOCOL (IP) ADDRESSES FOR LOCAL IP HOTLISTS.

2A(11). MEASURE A-11: UPDATE INDICATIONS AND WARNING ATTACK

SIGNATURES, PROFILES, AND METHODS OF RECENT ATTACK FOR USE BY INTRUSION DETECTION SYSTEMS, AND FOR USE BY SA TO MANUALLY DETECT INTRUSIONS.
2A(12). MEASURE A-12: SA WILL UPDATE ALL VIRUS SOFTWARE AND DAT FILES. ALL WORKSTATIONS WILL BE SCANNED FOR VIRUSES.
PAGE 07 RUEASRB0870 UNCLAS
2A(13). MEASURE A-13: SA WILL VALIDATE THE OPERATION OF SERVER SYSTEM LOG FILES, AND IN ADDITION TO DAILY REVIEWS, REVIEW FIREWALL AND INTRUSION DETECTION LOGS FOR EVIDENCE OF SPECIFIED UNUSUAL OR MALICIOUS ACTIVITY.
2A(14). MEASURE A-14: SA WILL ENSURE ROUTERS AND FIREWALLS PROTECTING ALL SEGMENTED CRITICAL C4I NETWORKS HAVE PROPER CONFIGURATION SETTINGS TO GUARD AGAINST KNOWN VULNERABILITIES AND METHODS OF RECENT ATTACKS.
2A(15). MEASURE A-15: ONCE A MONTH, REMIND ALL USERS TO PERFORM A STU-III KEY UPDATE.
2A(16). MEASURE A-16: ISSO-ISSM LOCATE AND VERIFY CURRENT STATUS OF ALL ACCREDITATION PACKAGES.
2A(17). MEASURE A-17: ENSURE THAT THERE ARE LOCAL PROCEDURES TO ASSESS AND IMPLEMENT THE DIRECTIVES STATED IN THE INFORCON MESSAGE IN THE TIMEFRAME REQUIRED. THIS INCLUDES PROCEDURES TO CONTACT KEY INFORMATION ASSURANCE PERSONNEL AFTER DUTY HOURS.
2B. INFOCON BRAVO.
2B(1). MEASURE B-1: ENSURE ALL ALPHA MEASURES ARE IMPLEMENTED AS DIRECTED.
2B(2). MEASURE B-2: DIRECT ALL ISSM, ISSO AMD SA TO INCREASE THEIR
PAGE 08 RUEASRB0870 UNCLAS
SECURITY AWARENESS, PARTICULARLY FOR CRITICAL C4I SYSTEMS, AND PLACE THEM ON ALERT FOR POSSIBLE RECALL AFTER NORMAL DUTY HOURS.
2B(3). MEASURE B-3: CLOSE ALL REMOTE MAINTENANCE PORTS ON VULNERABLE OR AFFECTED ROUTERS, FIREWALLS, SERVERS, COMPUTER-BASED TELEPHONE SWITCHES, AND ANY OTHER ACCESSIBLE INFORMATION SYSTEMS.
2B(4). MEASURE B-4: SA WILL REDUCE DIAL IN ACCESS TO MINIMUM ESSENTIAL PERSONNEL AS DIRECTED BY DCSOPS/G3.
2B(5). MEASURE B-5: NOTIFY POST, CAMP, STATION LAW ENFORCEMENT AND EMERGENCY PERSONNEL OF INFOCON STATUS.
2B(6). MEASURE B-6: SA WILL REVIEW NETWORK MONITORING LOGS, SYSTEM AUDIT LOGS, AND SERVER SYSTEM LOG FILES FOR EVIDENCE OF SPECIFIED UNUSUAL OR MALICIOUS ACTIVITY.
2B(7). MEASURE B-7: DEVELOP FINAL PLAN FOR CONFIGURATION SETTINGS

FOR FIREWALLS, ROUTERS, FILTERS, AND GUARDS FOR INFOCON CHARLIE IMPLEMENTATION.
3. FORSCOM POCS ARE LTC TALKINGTON, AFOP-OCF, DSN: 367-5709, EMAIL: TALKINGDN(AT)FORSCOM.ARMY.MIL AND LTC PERKINS, AFCI-J, DSN: 367-7515, EMAIL: PERKINSNW(AT)FORSCOM.ARMY.MIL.//
BT
#0870

NNNN

ANNEX H (VIRUS DESCRIPTION) TO “ILOVEYOU” VIRUS LESSONS LEARNED REPORT

“ILOVEYOU” VIRUS DESCRIPTION

The ILOVEYOU or Love Letter worm is a visual basic script that comes in an email. The text of the email asks you to open the attachment called LOVE-LETTER-FOR-YOU.TXT.vbs. Opening this attachment will cause the script to execute.

The script does several things:

1. it sends an email to everyone in your address book forwarding the attachment (this only works on MS Outlook and Outlook Express).
2. it attempts to connect to a web site and down load two additional files (WinFAT32.EXE and WIN-BUGSFIX.EXE). These files are downloaded by setting your Internet Explorer home page to the site where the files are located.
3. it sets registry entries so that MSKernel32.vbs, Win32DLL.vbs and WIN-BUGSFIX.EXE execute on start up. WIN-BUGFIX.exe file will then email any cached passwords to MAILME@SUPER.NET.PH."
4. it searches for all vbs, vbe, js, jse, css, wsh, sct, hta, jpg, jpeg, mp3, and mp2 files and replaces their contents with the Love letter script. It then adds a .vbs extension to all these files. This file replacement works on all local drives, all attached network drives, and (we have one report) that it also searches all "remembered" drives - i.e. drives that have been connected recently.

The script will work for email programs other than MS Outlook (such as Lotus Notes). The only part that does not work is the propagation via email.

ANNEX I (IAVA) TO "ILOVEYOU" VIRUS LESSONS LEARNED REPORT

INFORMATION ASSURANCE VULNERABILITY ALERT (IAVA)

APPENDIX 1 (FORSCOM IAVA PROGRAM) TO ANNEX I (IAVA) TO "ILOVEYOU" VIRUS LESSONS LEARNED REPORT

INFORMATION ASSURANCE VULNERABILITY ALERT (IAVA)

1. IAVA is a key mechanism of information system defense. In this process, the Army Computer Emergency Response Team (ACERT) notifies system administrators (SA) and other IA personnel of confirmed system/network vulnerabilities and associated "fixes." All FORSCOM installation IA POC's, system administrators and network managers must be registered with the ACERT to automatically receive Information Assurance Alerts, Bulletins and TechTips and comply with actions directed in ACERT-issued IAVA notices. Receipt of ACERT-issued Alerts & Bulletins must be acknowledged by FORSCOM installations to the FORSCOM DCSC4 IA Team. There are positive controls for acknowledging and reporting compliance to IAVA notifications.

2. HQ FORSCOM DCSC4 IA Branch. The responsibility at this level primarily consists of monitoring and reporting. Specific reporting requirements are listed in the "boiler plate" of the alert/advisory and includes two steps: (1) Acknowlege receipt of alert/advisory, (2) Provide summary report of actions taken by installations. Specific actions include:

- Ensure that installations are aware of requirement to acknowledge receipt of alert/advisory to the MACOM. Follow up with installation IA POC if acknowlegement is not received by the next working day after DCSC4 IA Branch opens the alert/advisory for tracking.

- Provide a summary of actions (IAW alert/advisory instructions) NLT suspense date. Do not delay reporting in order to include all installations. Provide followup report (i.e., information from late reporting installations) as necessary.

- Maintain a spreadsheet showing IAVA status.

3. Installations. The installations have reporting and "fixing" requirements. The steps include (1) report receipt to MACOM, (2) execute "fix" if applicable, and (3) report fix to MACOM. Specific actions include:

- Acknowledge receipt of alert/advisory to FORSCOM the same business day that it is received.

- Establish local procedures to ensure that this function (i.e., IAVA reporting) is covered during the absence of personnel with IAVA reporting responsibilities. This includes the assignment of alternates and procedures for requesting extensions (as necessary) prior to the suspense date.

4. We have established IA POCs at each installation that we deal directly with for IAVA reporting requirements. The installation POCs have a much more difficult job because they have to coordinate with all the SAs/NMs that are responsible for IAVA reporting. This includes those in tenant activities.

APPENDIX 2 (ARMY IAVA POLICY) TO ANNEX I (IAVA) TO "ILOVEYOU" VIRUS LESSONS LEARNED REPORT

FROM
:DA WASHINGTON DC//SAIS-IAS//
TO
:CDRUSAREUR HEIDELBERG
:GE//AEACG/AEADC/AEAGX/AEAIM/AEAGB/AEAGC//
:CDRAMC ALEXANDRIA VA//AMCCG/AMCIO-F/AMCIO//
:CDRFORSCOM FT MCPHERSON GA//AFCG/AFCS/AFIN/AFCI//
:CDRTRADOC FT MONROE VA//ATCG/ATIM/ATIM-I//
:CDRUSASOC FT BRAGG NC//CG/AOIM-SE/DCSIM//
:CDRUSACE WASHINGTON DC//CG/CECS-PM-ZC//
:CDRUSAMEDCOM FT SAM HOUSTON TX//CG/ACSIM//
:CDRUSARPAC FT SHAFTER HI//CG/DCSIM//
:CDRUSAEIGHT SEOUL KOR//CG/EAIM//
:SUPT USMA WEST POINT NY//MAIM//
:CNGB WASHINGTON DC//NGB-ZA/NGB-CIO//NGB-AIS//
:ARNGRC ARLINGTON VA//NGB-AIS/AIS-TS//
:CDRUSASMDC ARLINGTON VA//CG/DCSIM//
:CDRUSAIGA WASHINGTON DC//SAIG-IR//
:CDRMTMC FALLS CHURCH VA//MTCG/DCSIM//
:CDRUSAMDW FT MCNAIR WASHINGTON DC//ANCG/ANIM-IMS//
:CDRUSARSO FT CLAYTON PM//SOCG/SOIM//
:OCAR WASHINGTON DC//DAAR-ZA//
:CDRUSARC FT MCPHERSON GA//CG/AFRC-CIS/AFRC-CII//
:CDRPERSCOM ALEXANDRIA
:VA//TAPC-ZA/TAPC-PSP/TAPC-ALC/DCSIM//
:CDRUSAREC FT KNOX KY//RCCG/DCSIM//
:CDROPTEC ALEXANDRIA VA//CSTE/DCSIM//
:CDRINSCOM FT BELVOIR VA//IACG/IAIM-M//
:CDRUSACIDC FT BELVOIR VA//CICG-ZA/CICG-SC/DCSIM//
:DCDRUSASMDC HUNTSVILLE AL//DCSIM-A/SMDC-IM//
:PEO AVN REDSTONE ARS AL//SFAE-AV/DCSIM//
:PEO GCSS PICATINNY ARSENAL NJ//SFAE-GCSS/DCSIM//
:PEO C3S FT MONMOUTH
:NJ//SFAE-C3S/SFAE-C3S-PMO/SFAE-C3S-REO/SFAE-C3S-STR-STA
:/SFAE-C3S-TRC/SFAE-C3S-TRC-TMD/SFAE-C3S-WIN/SFAE-C3S-WI
:N-AMD/SFAE-C3S-WIN-CMS/SFAE-C3S-WIN-FMS/SFAE-C3S-WIN-RR
:D/SFAE-C3S-WIN-RRD-A/SFAE-C3S-WIN-TMD/SFAE-C3S-XO/AMSEL
:-DSA-GPS/DCSIM//
:PEO AIR AND MISSLE DEFENSE REDSTONE ARS
:AL//SFAE-AMD/DCSIM//
:PEO STAMIS FT BELVOIR VA//SFAE-PS//
:PEO IEW FT MONMOUTH
:NJ//SFAE-IEW/SFAE-IEW-D/SFAE-IEWS-JS-BMD/SFAE-IEWS-JTT/
:SFAE-IEWS-JTT-BMD/SFAE-IEWS-NV-TS/SFAE-IEWS-NV-TS-BMD/S
:FAE-IEWS-SG/SFAE-IEWS-SG-BMD/SFAE-IEW-CI/DCSIM//
:PEO TACTMSL REDSTONE ARS AL//SFAE-MSL/DCSIM//

:PM JCALS FORT MONMOUTH NJ//SFAE-PS-CAL/SFAE-PS-CAL-S//
:PM DMS-ARMY FT MONMOUTH NJ//SFAE-PS-DMS//
:USARSPACE COLORADO SPRINGS CO//DCSIM//
:DIRLIWA FT BELVOIR VA//LIWA-DR/DCSIM//
:CDRUSASC FT HUACHUCA AZ//AFSC-CG/DCSIM/AFSC-IS//
:CDR5THSIGCMD MANNHEIM GE//AFSE-IS//
:CDR516THSIGBDE FT SCHAFTER HI//CDR//
:CDR1STSIGBDE SEOUL KOR//AFSK-C//
:COMDT USAWC CBKS PA//AWCC-SAS//
:CDRUSACFSC ALEXANDRIA VA//ZA/CFSC-IM/CFSC-IM-IA//
:RHHJRAP/USARPAC INTEL FT SHAFTER HI//APIN-SC//
:CDR CECOM FT MONMOUTH
:NJ//AMSEL-DSA-GPS-B-G-R/AMSEL-DSA-AF/AMSEL-DSA-TS-AS/AM
:SEL-DSA-TSB/AMSEL-DSA-TSB-A/AMSEL-DSA-TSD/AMSEL-DSA-TST
:/AMSEL-DSA-TSU//
:CDR USA EIGHT SEOUL KOREA//EAIM-C-C4//
:DA WASHINGTON
:DC//DAMO-ZA/SAIS-ZA/DAMI-ZA/SARD-ZA/SAIG-ZA/SAM-ZA/
:SAIS-ZA/SAIE-ZX/DALO-ZX/DAPE-ZX/DAEN-ZX/DAMO-TR/
:JDIM-RM/DAJA-ZX/DAZG-ZX/SAAA-ZX/SAPA-ZX/DAIM-ZB/
:DACS-ZC//
INFO
:SECDEF WASHINGTON DC//ASD C3I/IIA/DIAP//
:DA WASHINGTON
:DC//DAMO-ODI/DAMO-TRO/DAMI-POD/DAMI-IM/DAMI-CH/SAIS-IAS
:/DAMO-FD/SAIS-PAA-M/SAIS-PA/SAIS-IM//
:DISA GOSC WASHINGTON DC//D3/D3113//
:JOINT STAFF WASHINGTON DC//J6K/J6T/J39//
XMT
:
ACCT
:
TEXT
:UNCLAS
SUBJECT: NETWORK SECURITY IMPROVEMENT PROGRAM (NSIP): ARMY POLICY FOR THE IMPLEMENTATION OF THE INFORMATION ASSURANCE VULNERABILITY (IAVA) PROCESS.
REFERENCE:
A. SECDEF MESSAGE DTG 252016ZJUN98, SUBJECT: INFORMATION ASSURANCE VULNERABILITY ALERT PROCESS
B. SAIS-IAS MESSAGE DTG 271633Z MAY 98, SUBJECT: IMPLEMENTING INFORMATION ASSURANCE (IA) VULNERABILITY ALERT/POSITIVE CONTROL IN SUPPORT OF ARMY COMPUTER NETWORK DEFENSE
1. THE PURPOSE OF THIS MESSAGE IS TO CLARIFY AND EXPAND ARMY POLICY FOR THE IAVA PROCESS. THIS POLICY APPLIES TO THE ACTIVE ARMY, THE ARMY NATIONAL GUARD, AND THE U.S. ARMY RESERVE.

2. REFERENCE A. ABOVE PROMULGATED DOD POLICY FOR IMPLEMENTING IAVA. THIS MESSAGE TASKED EACH SERVICE WITH ESTABLISHING "POSITIVE CONTROL" OVER THEIR SYSTEMS AND NETWORKS. AS STATED IN REFERENCE B. ABOVE, THE CHIEF INFORMATION OFFICER (CIO) OF THE ARMY IS RESPONSIBLE FOR EXECUTING "POSITIVE CONTROL" BY ENSURING A MEANS FOR (1) VULNERABILITY IDENTIFICATION, DISSEMINATION, AND ACKNOWLEDGMENT; (2) COMPLIANCE REPORTING; AND (3) COMPLIANCE VERIFICATION. THE CIO IS DESIGNATED AS THE ARMY POC TO ACKNOWLEDGE RECEIPT (WITHIN FIVE DAYS) OF DEFENSE INFORMATION SYSTEMS AGENCY (DISA) ISSUED IAVA MESSAGES, TO AGGREGATE COMPLIANCE AND WAIVER DATA, AND TO REPORT THE SERVICE STATUS TO DISA. IN ADDITION, THE ACERT/CC AGGREGATES MACOM/PEO/PM COMPLIANCE REPORTING DATA ON ALL IAVA MESSAGES AND PROVIDES REPORTS TO THE ODISC4 ARMY IA OFFICE, THE ARMY CIO AND ARMY SENIOR LEADERSHIP.

3. THE CIO OF THE ARMY (THE DIRECTOR OF INFORMATION SYSTEMS FOR COMMAND, CONTROL, COMMUNICATIONS, AND COMPUTERS [DISC4]), AND THE ARMY DEPUTY CHIEF OF STAFF FOR OPERATIONS AND PLANS (DCSOPS) DESIGNATED THE LAND INFORMATION WARFARE ACTIVITY'S (LIWA) ARMY COMPUTER EMERGENCY RESPONSE TEAM COORDINATION CENTER (ACERT/CC) AS THE ARMY'S FOCAL POINT FOR IMPLEMENTATION OF THE IAVA PROCESS.

4. ACERT/CC ISSUES ALERTS AND ADVISORIES VIA THE ACERT/CC LISTSERV ON BEHALF OF THE CIO AND THE DCSOPS OF THE ARMY. TO PROVIDE REDUNDANCY, IAVA ALERTS AND ADVISORIES ARE ALSO DISSEMINATED VIA GENERAL SERVICE (GENSER) MESSAGE AND THE ODISC4 IA EMAIL DISTRIBUTION LIST. THESE MESSAGES ARE BASED ON BOTH MANDATORY DISA ISSUED IAVA MESSAGES AND ARMY GENERATED IAVA REQUIREMENTS. ACERT/CC IAVA MESSAGES DIRECT SPECIFIC ACTIONS AND GIVE MANDATORY SUSPENSE DATES FOR COMPLIANCE. IF A MACOM/PEO/PM CANNOT MEET THE SUSPENSE FOR COMPLIANCE, THEY MUST CONTACT THE ACERT/CC, COORDINATE A PLAN, AND SET A NEW DATE FOR COMPLIANCE. THE PLAN MUST PROVIDE A MIGRATION PATH WITH MILESTONES FOR A SECURITY SOLUTION APPROVED BY THE APPROPRIATE MACOM/PEO/PM DESIGNATED APPROVING AUTHORITY (DAA), AND THE PLAN MUST BE FORWARDED TO THE CIO OF THE ARMY (SEE ODISC4 POCS IN PARA 12) FOR APPROVAL. THE ACERT/CC, ON BEHALF OF THE ARMY CIO, MAY GRANT AN EXTENSION, BUT THE MACOM/PEO/PM DOES NOT HAVE THE OPTION OF NOT REPORTING ACKNOWLEDGEMENT AND COMPLIANCE. NOTE: THE CIO OF THE ARMY IS THE FINAL APPROVING AUTHORITY OF MIGRATION PLANS TO IMPLEMENT IAVA MESSAGES.

5. IT IS MANDATORY THAT ALL SYSTEMS ADMINISTRATORS, INFORMATION ASSURANCE/INFORMATION SYSTEM SECURITY PERSONNEL, NETWORK OPERATIONS PERSONNEL, AND FORCE PROTECTION PERSONNEL SUBSCRIBE TO THE ACERT/CC LISTSERV. THESE PERSONNEL CAN SUBSCRIBE TO THE LISTSERV VIA THE ACERT/CC WEBSITE SITE (HTTP://WWW.ACERT.BELVOIR.ARMY.MIL). WHILE THE ACERT/CC LISTSERV IS

THE OFFICIAL NOTIFICATION FOR IAVA COMPLIANCE REQUIREMENTS TO MACOM/PEO/PM LEVEL IAOS, IT IS INFO TO SUBORDINATE ELEMENTS UNTIL TASKED IN ACCORDANCE WITH (IAW) PROCEDURES ESTABLISHED BY THE MACOM/PEO/PM. LIKEWISE, COMPLIANCE REPORTING WILL BE ACCOMPLISHED IAW MACOM/PEO/PM IAVA PROCEDURES. THE MACOM/PEO/PM INFORMATION ASSURANCE OFFICER (IAO) WILL REPORT THE COMMAND'S ACKNOWLEDGEMENT AND COMPLIANCE STATUS TO THE ACERT/CC.

6. THE INFORMATION ASSURANCE (IA) OFFICER FOR EACH MACOM/PEO/PM IS RESPONSIBLE FOR:

A) REPORTING THE ACKNOWLEDGEMENT OF THE IAVA MSG TO THE ACERT/CC, USUALLY WITHIN 5 DAYS.

B) PROVIDING THE COMMANDER'S GUIDANCE TO SUBORDINATE UNITS/ORGANIZATIONS/ACTIVITIES/ELEMENTS/PROGRAMS AND ENSURING THE MACOM/PEO/PM CHAIN OF COMMAND IA OFFICERS COMPLY WITH IAVA REQUIREMENTS.

C) REPORTING MACOM/PEO/PM COMPLIANCE STATUS. BOTTOM LINE: THE MACOM/PEO/PM IAO IS RESPONSIBLE FOR REPORTING THE COMMAND'S IAVA ACKNOWLEDGEMENT AND COMPLIANCE STATUS TO THE ACERT/CC.

D) ENSURING INSTALLATION/UNIT IA OFFICERS AND INSTALLATION/UNIT SYSTEM ADMINISTRATORS/NETWORK MANAGERS COORDINATE WITH PEOS/PMS PRIOR TO TAKING ACTION ON ALERTS THAT ADDRESS VULNERABILITIES ON PLATFORMS UNDER PEO/PM COGNIZANCE.

7. FOR NOCS AND CERTS ONLY: IF AN ATTACK TARGETS SERVERS AND THE NEED FOR A QUICK DISSEMINATION/RESPONSE NEGATES THE UTILITY OF GENSER MESSAGES, AN ADDITIONAL MEANS FOR DISSEMINATION MUST BE AVAILABLE. ALL ARMY NETWORK OPERATION CENTERS (NOC) AND ARMY COMPUTER EMERGENCY RESPONSE TEAMS (CERTS) MUST MAINTAIN A DATABASE THAT WILL PROVIDE THE NOCS AND CERTS THE ABILITY TO CONTACT KEY NOC AND CERT PERSONNEL TELEPHONICALLY. THIS WILL BE THE PRIMARY BACK-UP FOR DISSEMINATION OF IAVA INFORMATION.

8. COMMANDERS/DIRECTORS AT ALL LEVELS ARE RESPONSIBLE FOR THE ACCURACY OF THEIR IAVA REPORTING FOR ENSURING THAT ALL SUBORDINATE UNITS RECEIVE THE IAVA INFORMATION, THAT THE DIRECTED "FIX" IS IMPLEMENTED, AND THAT THE MACOM/PEO/PM COMPLIANCE STATUS IS REPORTED TO THE ACERT/CC AS OUTLINED IN PARAGRAPH 5, THIS MESSAGE.

9. MACOMS/PEOS/PMS HAVE THE OPTION OF ALLOWING THE ACKNOWLEDGEMENT AND COMPLIANCE FOR THEIR SUBORDINATE UNITS TO BE REPORTED VIA ANOTHER MACOM WHEN THE SUBORDINATE UNITS ARE LOCATED IN A GEOGRAPHICALLY SEPARATED LOCATION.

A) HOWEVER, THE MACOM/PEO/PM MAY NOT DELEGATE THE ACKNOWLEDGEMENT AND COMPLIANCE RESPONSIBILITIES OF THEIR SUBORDINATE ELEMENTS.

B) SUBORDINATE ELEMENTS IN A GEOGRAPHICALLY SEPARATED AREA MAY HAVE THEIR COMPLIANCE AND REPORTING INFORMATION ROLLED UP INTO

THEIR HOST'S SITE REPORT ONLY AFTER THERE HAS BEEN MACOM/PEO/PM IAO TO MACOM/PEO/PM IAO COORDINATION AND AGREEMENT ON HOW THE ACKNOWLEDGEMENT AND COMPLIANCE DATA WILL BE REPORTED TO THE ACERT/CC.

10. PEOS/PMS HAVE THE SAME RESPONSIBILITIES THAT A MACOM HAS TO REPORT ACKNOWLEDGEMENT AND COMPLIANCE STATUS FOR ALL SUBORDINATE UNITS/ELEMENTS/ACTIVITIES/PROGRAMS WITHIN THEIR LIFE CYCLE SUPPORT AUTHORITY.

A) PEOS/PMS MUST ENSURE THAT SUBORDINATE UNITS/ELEMENTS/ ACTIVITIES/PROGRAMS MAINTAIN A CONFIGURATION BASELINE ON SYSTEMS FOR WHICH THEY HAVE POST PRODUCTION SOFTWARE SUPPORT (PPSS) RESPONSIBILITIES.

B) THE PEO/PM IS RESPONSIBLE FOR COMPARING IAVA MESSAGES AGAINST SYSTEM BASELINES AND TAKING APPROPRIATE ACTION TO ENSURE THE SYSTEM MEETS THE IAVA DIRECTED STANDARD.

C) NO PEO/PM HAS A WAIVER THAT EXEMPTS FIELDED/IN DEVELOPMENT SYSTEMS FROM MEETING IAVA STANDARDS. IF A SYSTEM CANNOT MEET THE IAVA STANDARD WITHIN THE SUSPENSE, THEN A WAIVER MUST BE SENT TO THE ODISC4 POC THIS MESSAGE. IN ORDER TO CONSIDER THE WAIVER, A MIGRATION PLAN WITH MILESTONES THAT OUTLINES HOW THE SYSTEM WILL MEET THE IAVA REQUIREMENT MUST BE ATTACHED.

D) THE PEO/PM IS ALSO RESPONSIBLE FOR ENSURING THAT THE IAVA MESSAGES ARE DISSEMINATED TO ALL UNITS/ELEMENTS/ACTIVITIES/PROGRAMS THAT ARE DEVELOPING SYSTEMS AND ENSURE THAT IAVA DOCUMENTED VULNERABILITIES ARE CORRECTED PRIOR TO FIELDING.

11. TO MEET THE DEPUTY SECRETARY OF DEFENSE (DEPSECDEF) IAVA "POSITIVE CONTROL" COMPLIANCE REPORTING REQUIREMENTS, ALL MACOM/PEO/PM IAOS MUST ENSURE THAT SUBORDINATE IAOS AT EVERY ECHELON MAINTAIN A COMPLETE "LIST" (A DATABASE, SPREADSHEET, ETC) OF ALL SYSTEM ADMINISTRATORS AND NETWORK MANAGERS RESPONSIBLE TO THEM FOR IMPLEMENTING MANDATORY IAVA REQUIREMENTS, INCLUDING THEIR EMAIL ADDRESSES AND PHONE NUMBERS. WHILE THERE IS NO REQUIREMENT FOR MACOM/PEO/PM IAOS TO "ROLL UP" ALL DATA INTO A "MASTER LIST" FOR THE COMMAND, MACOM/PEO/PM IAOS MUST HAVE THE CAPABILITY TO QUERY EVERY SUBORDINATE IAO AND RECEIVE THEIR "LIST." HQDA IS AWAITING ADDITIONAL IAVA REPORTING GUIDANCE FROM THE OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE FOR COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE (OASDC3I) AND ANTICIPATES "POSTIVE CONTROL" COMPLIANCE REPORTING WILL INCLUDE BOTH THE NUMBER OF SERVERS AFFECTED AND THE NUMBER IN COMPLIANCE FOR WHICH SYSTEMS ADMINISTRATORS ARE RESPONSIBLE. ADDITIONAL INFORMATION WILL BE PROVIDED AS IT BECOMES AVAILABLE. THIS PROCESS AND/OR DATABASE MUST BE OPERATIONAL NLT 15 OCT 99.

12. DISC4 POLICY POCS FOR THIS MESSAGE ARE LTC ROY LUNDGREN, DSN:

664-8377, COM 703-706-8377, EMAIL LUNDGL@HQDA.ARMY.MIL OR PHILLIP LORANGER, DSN: 327-5887, COM 703-607-5887, EMAIL LORANPJ@HQDA.ARMY.MIL. TECHNICAL POLICY POCS FOR THIS MESSAGE ARE RON STURMER, DSN 664-6870, COM 703-604-6870, EMAIL: STURMRT@HQDA.ARMY.MIL; RALPH A. LOWENTHAL, DSN 327-5886, COM 703-607-5886 EMAIL LOWENRA@HQDA.ARMY.MIL.

ANNEX J (TRAINING REQUIREMENT) TO "ILOVEYOU" VIRUS LESSONS LEARNED REPORT

INFORMATION ASSURANCE TRAINING

APPENDIX 1 (KCI) TO ANNEX J (TRAINING REQUIREMENT) TO "ILOVEYOU" VIRUS LESSONS LEARNED REPORT

KCI

AFCI-JI | **LaBonte, Don - DCSC4 / 6467**
4/6/00

ISSUE: Information Assurance Training

POINTS:

- The Army recognizes that an informed and trained workforce is key to a good Information Assurance (IA) program and has established training criteria to ensure that Army personnel are "certified" to perform IA functions within their area of responsibility.

- User "awareness" training is developed and provided locally by the Information Assurance Managers (IAM) using materials readily available from DOD and other government sources.

- A two week Security lab for System Administrators (SA) and Network Managers at Fort Gordon trains personnel that have the responsibility to install, operate and maintain networks and information systems, how to recognize vulnerabilities and defend against threats by implementing information security procedures and technologies.

- IAM training sponsored by HQDA (DISC4) is designed to provide IAMs and their staffs the knowledge to identify the laws, directives and regulations relating to IA and implement and manage the Army information Assurance Program. In addition, FORSCOM has contracted with Georgia Tech to provide a 5-day course which addresses information dominance, INFOSEC, COMSEC, COMPUSEC, defense information warfare, information operations strategy, and defense information infrastructure.

STATUS: User IA awareness training is ongoing at all installations. DCSC4 hosted/is hosting the DISC4-sponsored Information Systems Security Manager (ISSM) course at Ft McPherson in Aug 99, Nov 99, Apr 00, and Sep 00. Each of these sessions "certifies" approximately 25 IA Managers. In addition, 40 IA professional have attended the GA Tech IA Managers course which we plan to offer again during CY00. SA training labs have been started up at McCoy, Huachuca and Hood, and Bragg and Lewis have been given funds to establish labs. Based on a Feb 00 data call, 122 SAs of a total requirement of 667 have attended this training.

FORSCOM POSITION: Continue to promote IA training.

APPENDIX 2 (CERTIFICATION REQUIREMENT) TO ANNEX J (TRAINING REQUIREMENT) TO "ILOVEYOU" VIRUS LESSONS LEARNED REPORT

R 061645Z MAY 98

FM PTC EMAIL SYSTEM WASH DC

INFO DA EMAIL CUSTOMER//DAMI/SAM-OPT/SAIS/CEHECIM//
R 060727Z MAY 98 PASS TO C2 PROTECT POCS

FM DA WASHINGTON DC//SAIS-PAC-I//

TO CDRUSARSPACECOM COLORADO SPRGS CO
CNGB WASHINGTON DC//NGB-ARL-S//
CDRUSAMTMC FALLS CHURCH VA//MTIM//
CDRUSACIDC FT BELVOIR VA//CIOP-IN-SC//
CDRUSASSDC HUNTSVILLE AL//CSSD-SA-T/T SMALL//
CDRUSARPAC FT SHAFTER HI//C2 PROTECT POC/N HARRISON//
CDRUSASOC FT BRAGG NC//ASOF-IM//
CDRUSACE WASHINGTON DC//CEIM//
CDRUSAEIGHT SEOUL KOR//C2PROTECT POC//
CDRINSCOM FT BELVOIR VA//IAIM-M//
CDRTRADOC FT MONROE VA//ATIM-M//
CDRUSAMEDCOM FT SAM HOUSTON TX//MCHO-OP-SI//
CDRUSARC FT MCPHERSON GA//AFRC-INS//
CDRUSAFORCES FT MCPHER GA//C2PROTECTPOC/HANKINS//
CDRUSAREC FT KNOX KY//RCIM-CE-IA//
DIRSAM PENTAGON WASHINGTON DC//SAM-ZA//
CDRUSASOUTH FT CLAYTON PN//D 2PROTECT POC//
SUPDT USMA WEST POINT NY//C2 PROTECT POC-TRIMBLE//
CDR5THSIGCMD WORMS GE //DCSINT/COL TREECE//
CDRUSASC FT HUACHUCA AZ//AFSC-IS//
CDRAMC ALEXANDRIA VA//AMCIO-F//

INFO DA WASHINGTON DC//DAMO-ODI/DAMI-POD/DAMI-IM/DAMI-CH//
DISAGOSC WASHINGTON DC //D33//
DA WASHINGTON DC//DAMO-TRO//
JOINT STAFF WASH DC//J6K//

UNCLAS

SUBJECT: SECURITY LICENSING FOR PERSONNEL WHO USE, ADMINISTER, MANAGE, AND SECURE DEPARTMENT OF THE ARMY (DA) INFORMATION SYSTEMS AND NETWORKS REFERENCES:
A: JOINT STAFF, J6K DRAFT MEMORANDUM, SUBJECT: LICENSING OF PERSONNEL USING, ADMINISTERING, AND SECURING DEPARTMENT OF DEFENSE (DOD) INFORMATION SYSTEMS AND NETWORKS DATED 1 OCTOBER 1997.
B: DA MSG, DTG:101320Z MAR 98, SECURITY TRAINING FOR SYSTEMS

ADMINISTRATORS AND NETWORK MANAGERS

1. THE ARMY CHIEF INFORMATION OFFICER (CIO), THROUGH THE ARMY INFORMATION ASSURANCE OFFICE, COMMAND AND CONTROL PROTECT (C2 PROTECT) DIVISION, IS INSTITUTING A PROGRAM, IN ACCORDANCE WITH THE INTENT OF REFERENCE A, TO LICENSE ALL USERS/OPERATORS; INFORMATION SYSTEM SECURITY OFFICERS (ISSO), INFORMATION SYSTEM SECURITY MANAGERS (ISSM), AND INFORMATION SYSTEM SECURITY PROGRAM MANAGERS (ISSPM); AND SYSTEM ADMINISTRATORS AND NETWORK MANAGERS. CURRENT LICENSING CRITERIA FOR EACH CATEGORY ARE OUTLINED IN PARAGRAPH 3.

2. ALL PERSONNEL OPERATING ON DOD INFORMATION SYSTEMS AND NETWORKS WILL BE LICENSED BY DECEMBER 2000 (REFERENCE A). AS STATED IN REFERENCE B, SYSTEM ADMINISTRATORS FOR THE GLOBAL COMMAND AND CONTROL SYSTEM (GCCS) (FIRST PRIORITY) AND THE SECURE INTERNET PROTOCOL ROUTER NETWORK (SIPRNET) MUST BE LICENSED BY JANUARY 1999. ADDITIONALLY, ORGANIZATIONS MUST BEGIN PROGRAMMING NOW FOR THE RESOURCES TO IMPLEMENT LICENSING TRAINING. NOTE: TDY COSTS TO ATTEND THE DIRECTOR OF INFORMATION SYSTEMS FOR COMMAND, CONTROL, COMMUNICATIONS, AND COMPUTERS (DISC4) MANAGED ISSO AND ISSM COURSES, THE DEFENSE INFORMATION SYSTEMS AGENCY (DISA) MANAGED ISSO COURSE, AND THE ARMY COMPUTER SCIENCE SCHOOL'S SYSTEM ADMINISTRATOR AND NETWORK MANAGER SECURITY COURSES (SEE PARAGRAPH 3 FOR DETAILS) ARE THE RESPONSIBILITY OF THE ATTENDEE'S ORGANIZATION.

3. PENDING SUBSEQUENT REFINEMENT OF SECURITY LICENSING CRITERIA RESULTING FROM RESPONSES TO PARAGRAPHS 3B(3) AND 3C, THE CURRENT CRITERIA FOR THE ARMY SECURITY LICENSING PROGRAM ARE:

A. USER/OPERATOR CATEGORY: THE DISA INFOSEC AWARENESS CD ROM DISK, SUPPLEMENTED WITH LOCALLY PROVIDED SYSTEM SPECIFIC SECURITY TRAINING, EXEMPLIFIES TRAINING THAT MEETS THE MINIMAL USER/OPERATOR LICENSING CRITERIA. ACTIVITIES MAY DEVELOP LIKE TRAINING TO THE DISA INFOSEC AWARENESS CD ROM DISK. LICENSES WILL BE GRANTED UPON SUCCESSFUL COMPLETION OF LOCALLY PROVIDED INFORMATION SYSTEMS SECURITY (ISS) AWARENESS TRAINING THAT MEETS THE ABOVE CRITERIA. USERS/OPERATORS MUST RECEIVE TRAINING PRIOR TO ISSUANCE OF A PASSWORD FOR NETWORK ACCESS. THE PASSWORD WILL CONSTITUTE PROOF OF LICENSING. SEE WEBSITE WWW.DISA.MIL/CISS THEN CLICK THE INFOSEC EDUCATION, TRAINING, AWARENESS, AND PRODUCTS BRANCH BUTTON AND THE PRODUCTS ORDER FORM HOTLINK FOR INFORMATION ON ACQUIRING THE CD ROM.

B. ISS STAFF (ISSO/ISSM/ISSPM) CATEGORY:

APPENDIX 2 (CERTIFICATION REQUIREMENT) TO ANNEX J (TRAINING REQUIREMENT) TO "ILOVEYOU" VIRUS LESSONS LEARNED REPORT

(1) ISSO: DISC4 AND DISA OFFER ISSO COURSES THAT FULFILL TRAINING AND LICENSING REQUIREMENTS. LICENSES WILL BE GRANTED UPON SUCCESSFUL COMPLETION OF THE DISC4 OR DISA MANAGED COURSES. CERTIFICATES OF COMPLETION AND APPOINTMENT ORDERS WILL CONSTITUTE PROOF OF LICENSING. SEE WEBSITE WWW.ARMY.MIL/DISC4/ISEC/C2P/C2PTNG.HTM FOR FURTHER INFORMATION ON DISC4 COURSE REQUIREMENTS AND AVAILABILITY.

(2) ISSM/ISSPM: ISSM AND ISSPM TRAINING/LICENSING CRITERIA MUST BE BASED ON THE REQUIREMENTS OUTLINED IN AR 380-19, INFORMATION SYSTEMS SECURITY. THE DISC4 OFFERS AN ISSM COURSE THAT FULFILLS TRAINING AND LICENSING REQUIREMENTS FOR ISSMS AND ISSPMS. THE COURSE IS ALSO AVAILABLE TO THEIR SUPPORTING STAFFS. LICENSES WILL BE GRANTED UPON SUCCESSFUL COMPLETION OF THE DISC4 MANAGED COURSE. CERTIFICATES OF COMPLETION AND APPOINTMENT ORDERS WILL CONSTITUTE PROOF OF LICENSING. SEE WEBSITE WWW.ARMY.MIL/DISC4/ISEC/C2P/C2PTNG.HTM FOR FURTHER INFORMATION ON COURSE REQUIREMENTS AND AVAILABILITY.

(3) IN ADDITION, SEVERAL MACOMS OFFER COURSES THAT CAN MEET THE ISSO/ISSM/ISSPM LICENSING CRITERIA. THE DISC4 C2 PROTECT TRAINING WORKING GROUP HAS BEEN TASKED TO REVIEW EXISTING ARMY COURSES FOR THEIR APPLICABILITY IN MEETING LICENSINGOBJECTIVES. THIS MESSAGE SOLICITS FROM ALL ARMY MACOMS INFORMATION ON ANY COURSES AND/OR PROGRAMS THAT ARE CURRENTLY IN PLACE OR UNDER DEVELOPMENT THAT CAN BE USED IN ACHIEVING THESE ISSO/ISSM/ISSPM LICENSING REQUIREMENTS. THOSE COURSES MEETING THE REQUIREMENTS WILL BE INCORPORATED INTO THE LICENSING PROGRAM. MACOM POCS ARE REQUESTED TO PROVIDE THE DISC4 C2 PROTECT TRAINING WORKING GROUP THE FOLLOWING INFORMATION ON ANY SUCH COURSES AND/OR PROGRAMS: COURSE TITLE, LENGTH OF COURSE, NUMBER OF CLASSES TAUGHT PER YEAR, AND THE PROGRAM OF INSTRUCTION (POI).

C. SYSTEM ADMINISTRATOR/NETWORK MANAGER CATEGORY: SUCCESSFUL COMPLETION OF THE ARMY COMPUTER SCIENCE SCHOOL'S SYSTEMS ADMINISTRATOR AND NETWORK MANAGER SECURITY COURSES MEETS THE LICENSING CRITERIA. CERTIFICATES OF COURSE COMPLETION WILL CONSTITUTE PROOF OF LICENSING. SEE WEBSITE WWW.GORDON.ARMY.MIL/CSS FOR FURTHER INFORMATION ON COURSE REQUIREMENTS. GIVEN THE VOLUME OF PERSONNEL REQUIRING SYSTEM ADMINISTRATOR/NETWORK MANAGER SECURITY CERTIFICATION, AND THE LIMITED NUMBER AND SIZE OF CLASSES, ADDITIONAL CERTIFICATION OPTIONS ARE UNDER CONSIDERATION AND THE C2 PROTECT TRAINING WORKING GROUP WILL ENTERTAIN ANY RECOMMENDATIONS MACOMS HAVE ON THIS ISSUE.

4. DISC4 POINTS OF CONTACT ARE MS. BAILEY, TELEPHONE (703) 607-5890,EMAIL: BAILEPE@HQDA.ARMY.MIL AND MR. LORANGER, TELEPHONE (703) 607-5887, E-MAIL LORANPJ@HQDA.ARMY.MIL.

APPENDIX K (MS4X FUNDING) TO “ILOVEYOU” VIRUS LESSONS LEARNED REPORT

FORSCOM MS4X Requirements ($K)

	FY01	FY02	FY03	FY04	FY05	FY06	FY07
FORSCOM	**7868**	**7169**	**7325**	**7489**	**7660**	**7840**	**8028**
ASC	**17846**	**18738**	**19676**	**20659**	**21692**	**22776**	**23916**
TOTAL	**25714**	**25907**	**27001**	**28148**	**29352**	**30616**	**31944**

The FORSCOM Information Assurance (IA) program was established to meet HQDA requirements for Information Assurance Vulnerability Alert (IAVA) reporting and to manage implementation of the FORSCOM Network Security Improvement Program (NSIP) Action Plan. All programs, procedures and policies that are designed to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality and non-repudiation are included under the IA Program umbrella. The Army Signal Command (ASC) is responsible for Echelons Above Corps (EAC) networks world-wide to include IA requirements related to the installation, operation and sustainment of these networks. ASC is also the Army Executive Agent for the following IA functions: provides a world-wide network view, develops and maintains the top-level security architecture, conducts operational assessments of IA tools, and implements IA initiatives such as regional proxy web servers. To date, FORSCOM has not received MS4X funding necessary to meet the Information Assurance requirements mandated by HQDA and has had to divert funds from other operational programs.