BY ORDER OF THE COMMANDER
30TH SPACE WING

30TH SPACE WING INSTRUCTION 33-120

1 MAY 2004

Communications

NOTICE TO AIRMEN AND INFORMATION ASSURANCE VULNERABILITY ALERT (NOTAM/IAVA) PROCEDURES

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at: **http://www.e-publishing.af.mil.**

OPR: 30 SCS/SCBC (MSgt William Martin) Certified by: 30 SCS/CC (Lt Col Alan Claypool)
Pages: 2
Distribution: F

This instruction is issued to establish policy for the reporting of NOTAMs/IAVAs. This extends the policy in Air Force Security System Instruction, AFSSI 5021, ***Time Compliance Network Order (TCNO) Management And Vulnerability And Incident Reporting.***

1. Responsibility: All personnel assigned as Workgroup Managers (WMs) and Information Systems Security Officers (ISSOs) are responsible for compliance with the procedures contained herein.

2. Policy: All groups, wing staff, and tenant units will appoint an ISSO and alternate. The ISSO is the single point of contact for all issues concerning NOTAMs/IAVAs. The Wing Computer Network Defense (WCND) office will coordinate directly with ISSOs.

2.1. When the WCND office receives a new NOTAM/IAVA, it will be sent out to all WMs and ISSOs. All WMs will report compliance numbers to their ISSO, who in turn reports compliance to WCND. WMs will stay up-to-date on all required training needed to ensure they properly fulfill their duties.

3. Procedures: A unit compliance date (UCD) will be established 7 days prior to NOSC completion date (NCD). Each group/unit will report NOTAM/IAVA compliance NLT noon on the UCD. NOTAMs/IAVAs with a short suspense may not allow for 7 days, and WCND will establish a due date and advertise accordingly.

3.1. As groups/units report compliance, WCND will scan their subnets to verify compliance. A report will be sent back to the group/unit listing computers that are still non-compliant. WCND will continue to scan each group/unit until 100% compliance is attained. Computers that have been patched and still show up as non-compliant will be worked individually between the unit and the WCND office.

3.2. At noon on the unit compliance date, WCND will send notification via email to all ISSOs who have not reported compliance with a courtesy copy 30SCS/CC.

3.3. The day following the unit compliance date, WCND will send notification via email to 30SCS/CC containing updated list of groups still non-compliant. 30SCS/CC will notify the 30OG/CC and all group and tenant commanders of compliance status.

3.4. Each day until the day before NCD, 30SCS/CC will receive an updated list of groups non-compliant. 30OG/CC and all group and tenant commanders will continue to be notified daily. If units are still non-compliant the day prior to NCD, 30SW/CC will be notified.

3.5. Groups that are non-compliant after the NCD will have all non-compliant computers removed from the network.

3.6. Computers will not be added back to the network until patches are loaded and vulnerability verified by WCND.

FRANK GALLEGOS, Colonel, USAF
Commander