

**Title IV Wide Area Network (TIVWAN)
Corrective Action Plan,
September 2000**

No	Control Area	Observation	Concur with Observation	Corrective Action / Description	Completion Date	Point of Contact
1	Security Life Cycle Planning	There was no evidence of appropriate security controls for the Maintenance, Disposal, and Authorization phases of the System Development Life Cycle.		Ensure that (as appropriate) privacy and security in the information life cycle are addressed in TIVWAN life cycle planning documents. See the Security Life Cycle Planning section for additional details.		
2	Authorize Processing	Although TIVWAN has not sought certification, this report could serve as the basis for a system certification/ authority to operate.		Obtain an IATO for one year from the OCIO as soon as practical. Within eighteen months from issuance of the IATO, perform a formal TIVWAN certification test under NIST guidance (FIPS 102).		
3	Central Security Focus/ Assigned Responsibility	<p>The ACSO is not appointed in writing. The ACSO has not attended an ACSO meeting regularly and the ACSO does not have an alternate to attend in his/her place.</p> <p>Conflicts have arisen over TIVWAN security controls and methods for implementation.</p> <p>Conflicts exist among TIVWAN, OPE, and TIVWAN applications management regarding what controls are required, who is responsible for implementing them, and how to best implement controls exist.</p> <p>Separation of duties for individuals with security responsibilities is achieved only partially.</p> <p>Security personnel lack adequate training in technology and IT security</p>		<p>Ensure the TIVWAN SSO is properly trained and qualified. See the section on security training and awareness, and the related recommendations for the Promote Awareness phase of the risk management cycle.</p> <p>In addition, a long-term computer security strategy, a compliance program, and descriptions of any liaison function for either external or intraorganizational entities should be documented.</p>		

No	Control Area	Observation	Concur with Observation	Corrective Action / Description	Completion Date	Point of Contact
		necessary to evaluate operational anomalies for security incidents or concerns.				
4	Security Awareness and Training	<p>The Functional Manager has had no systems security training.</p> <p>NCS does not have a security awareness or training program and no employees were identified as holding professional security certifications.</p> <p>Security issues are not given more attention. There is a perception at NCS that prosecutions for violations of the Privacy Act do not occur.</p>		Provide security training for the TIVWAN SSO; once trained, the TIVWAN SSO should assist the OCIO in setting up an entity-wide security awareness and training program. See the Security Awareness and Recommendations sections for detailed guidance.		
5	Rules of Behavior	Rules of behavior have not been documented specifically.		Document rules of behavior for TIVWAN. Ensure managers and users are trained to understand them.		
6	Personnel Security	<p>Security is not mentioned specifically in key ED and NCS personnel position descriptions.</p> <p>No specific procedures have been established for updates to personnel clearances/background investigations.</p> <p>No access termination statements have been established for departing or transferred NCS employees to certify their awareness of their continuing responsibility to safeguard data subject to the Privacy Act.</p> <p>No clarification as to whether or not the TIVWAN ACSO should be checking the SSN of the users against the NSLDS database to verif</p>		Implement ED personnel security guidance. See the Personnel Security section for additional details.		

No	Control Area	Observation	Concur with Observation	Corrective Action / Description	Completion Date	Point of Contact
		<p>if the user is in default on a student loan.</p> <p>306 forms are not stored in a secured area.</p> <p>GEIS staff are not provided feedback as to when they are cleared and at what level.</p>				
7	Application Software Maintenance Controls	<p>There was no evidence that controls were in place to protect against the illegal use of software.</p> <p>The Configuration Manager's training in CM has not included the full scope and responsibilities of a CM program.</p> <p>The end-user software does not indicate the last time and date of access to help them determine if anyone other than themselves has used the software.</p> <p>Programmers have had no training specific to IT security. Thus, it would be unlikely that they can identify vulnerabilities when making changes to software.</p> <p>Developers are allowed to move their own code from the test environment to the production environment using JCL statement. If any part of the JCL statement is missing (from using "cut & paste" method), it could mean that the test program could be run against the production database. If the test program changed many records, the repair could be costly.</p> <p>Developers, administrators, and svstems analvsts have access.</p>		<p>Examine ED guidance relating to system life cycle planning. Ensure that TIVWAN CM processes and procedures are consistent with that guidance, and that the TIVWAN SSO is integrated into the systems development and CM processes. SSO should be part of the approval chain for all proposed changes to system software.</p>		

No	Control Area	Observation	Concur with Observation	Corrective Action / Description	Completion Date	Point of Contact
		<p>update, and delete authority in all three databases used for TIVWAN (two test databases and one production database). Any member of the development group could create a program and bind it to the production database.</p> <p>NCS technical staff is not notified by GEIS prior to GEIS staff taking the system down for maintenance.</p> <p>It is unlikely that the institutions supported by TIVWAN are Y2K compliant, which could cause a failure in TIVWAN.</p>				
8	Identification and Authentication	<p>TIVWAN TG numbers are assigned to an institution. NSLDS assigns UserIDs to specific individuals. This creates a conflict between the TIVWAN and the NSLDS security procedures. TIVWAN performs no mapping or verification check between TIVWAN ID and NSLDS ID.</p> <p>Password dictionary checking is not performed to prevent users from choosing easily-guessed passwords (common passwords).</p> <p>Password resets are disproportionately high (300 per week for a community of 7,000 users).</p> <p>The Personal Identification Number (PIN) assignment, at the destination level, has yet to be implemented because of a lack of direction from</p>		<p>Ensure TIVWAN complies with SFA standards for data user IDs and passwords. See the Identification and Authentication Section above for detailed guidance.</p>		

No	Control Area	Observation	Concur with Observation	Corrective Action / Description	Completion Date	Point of Contact
		<p>the Government regarding its use. The PIN approach was developed as a cost-saving mechanism because of the volume of password resets required by customers. Implementation details yet to be resolved include how to provide the PIN to the individual.</p> <p>The Mark III system presents a vulnerability in that there are two times during the password change process when the passwords are stored as clear text (password change data are not compressed – only data are compressed). The first is when changing a password, the user submits the UserID, the old password, and the new password. A built-in password change procedure script signs the user onto the Mark III. The passwords are unencrypted until provided to Mark III, where they are encrypted for storage. The other is when the passwords are transferred to RACF, which is done in clear text, and then encrypted in RACF for storage.</p> <p>The password associated with the TG5 number can be changed easily. Individuals may call customer service or they may dial an automated voice response unit, enter their Z number and their TG5 number, and have their passwords reset. No additional information is required to provide assurance that the individual assigned to the TG5 number is the</p>				

No	Control Area	Observation	Concur with Observation	Corrective Action / Description	Completion Date	Point of Contact
		<p>one changing the password.</p> <p>The one-to-one ratio of TIVWAN UserIDs to mailboxes does not appear to fit structure needed by institutions.</p>				
9	Logical Access Controls	<p>Reassigning of UserIDs: TIVWAN's position is that the schools or the institutions own the UserIDs, not the official at the school to whom the ID is assigned or the various individuals who use the ID (listed at technical contact points). Schools are allowed to change technical contact points. NSLDS management has taken the view that the UserID is owned by the individual, not the institution. On April 25, 1997, a decision was reached that NSLDS would allow the contact point to be changed. Details of this decision were not yet available.</p> <p>When multiple UserIDs are assigned to one customer, they are assigned sequentially. Potentially, by using the IVR to reset a password, a user could make an error entering their customer ID and accidentally reset another user's password.</p> <p>Per NSLDS, NCS staff was putting incorrect TG5 numbers on the PA form. The basic reason for the incorrect information appears to be the failure to follow established procedures and poor quality control.</p> <p>NCS is accepting forms and assigning TG5 numbers to applicants who are not following the</p>		<p>Document and implement within one year TIVWAN-specific policies, standards, procedures and guidelines to govern logical access processes and mechanisms.</p>		

No	Control Area	Observation	Concur with Observation	Corrective Action / Description	Completion Date	Point of Contact
		<p>requirements for providing valid SSNs and DOBs.</p> <p>A recent concern within NSLDS is that UserIDs may not be switched from one person to another. TIVWAN is allowing this, so they switch to a new person, send E-Systems the LOA, and the NSLDS software rejects the application. The LOAs are on hold because there are no directions from the Government. NSLDS may allow the switch, but if they do, special action and recordkeeping will be required to maintain appropriate audit trails.</p> <p>E-Systems has started receiving the electronic destination point file. They are in the testing phase. Thus far, NSLDS has been unwilling to accept the file 100 percent with information as input - first they want to do comparison and reject non-matches. There is no estimated completion date for this comparison.</p> <p>If the Destination file was sent twice in one night, this would be noticed and addressed, although there are no official procedures that specify the number of files allowed to be sent/received per night.</p>				
10	Audit Trails	<p>Security-specific analysis has not been performed on the audit trail data.</p> <p>Audit trails are not created at the application level. There are no reports of specific commands.</p>		<p>Ensure TIVWAN audit results are being used effectively to help TIVWAN managers make appropriate risk decisions. See the Audit Trails and Recommendations sections for additional details.</p>		

No	Control Area	Observation	Concur with Observation	Corrective Action / Description	Completion Date	Point of Contact
		<p>The RACF audit function is not used to track the activities of selected (privileged) users.</p> <p>The Help Desk did not always verify that the caller was an authorized user by consistently checking to see if the caller is listed as the point of contact for the TG5 number.</p>				
11	Data Integrity / Validation Controls	<p>Security on mainframes – manufacturers of mainframes, such as IBM, provide a system integrity statement that defines their acceptance of responsibility for system integrity and describes the system changes that transfer that responsibility to the user.</p> <p>In the current PC/LAN environment, it is incumbent upon the user to establish and maintain effective system integrity controls.</p> <p>The TIV WAN environment is comprised of mainframes and PC/LAN components. Thus, its integrity controls must cover both environments. NCS has focused its mainframe system where controls are well-established, unintentionally overlooking the PC/LAN where threats and vulnerabilities are greater.</p>		<p>Ensure TIVWAN complies with SFA standards for data integrity and automated validations. See the Data Integrity section for additional details.</p>		
12	Physical and Environmental Protection	<p>The newly-designed regular employees' badges will not have an expiration date.</p> <p>The tape library is not separated by a firewall from the clean room, which poses additional risk.</p>		<p>When developing/updating the TIVWAN security plan, ensure the controls noted above are fully addressed.</p>		

No	Control Area	Observation	Concur with Observation	Corrective Action / Description	Completion Date	Point of Contact
		The section of the TIVWAN Security Plan that covers the physical security measures of GEIS does not provide specifics. The plan is also generalized and contains statements that need further clarifications.				
13	Production, Input/Output Controls	<p>The destination point file is provided nightly from NCS to NSLDS, but NSLDS is using paper documents instead. Changes to information on the forms by NCS staff should not be happening.</p> <p>Inappropriate information has been sent to schools. Documents reviewed showed changes, without any initials or names to provide accountability for who had made the changes. This is contrary to NCS procedures.</p> <p>Data is misdirected as a result of human error. This error has been compounded by a failure to follow established procedures, thereby eliminating the audit trail.</p>		Implement Security Life Cycle Planning, Authorize Processing and Application Software Maintenance Control recommendations; document input/output controls in the TIVWAN security plan.		
14	Documentation	<p>The Security Plan was not included for review.</p> <p>The computer Security Plan for TIVWAN was a one-time deliverable without a version number.</p> <p>The TIVWAN Security Plan does not meet the requirements of the Computer Security Act of 1987 and OMB Bulletin 90-08.</p>		Develop a NIST-compliant (Special Pub 800-18) security plan for TIVWAN. See the Recommendations section for additional details.		

No	Control Area	Observation	Concur with Observation	Corrective Action / Description	Completion Date	Point of Contact
15	Contingency Planning	<p>The Contingency Planning section of the Security Plan is potentially out-of-date and lacks documentation of detailed procedures. The emergency response operations sections are high-level.</p> <p>Copies of the plan are maintained in machine-readable (electronic) format at the off-site facility. Key personnel do not maintain printed copies of the plan at their homes.</p>		<p>Ensure formal contingency and incident response plans are consistent with NIST guidance (Special Pub 800-3). Ensure plans are exercised once annually, and the TIVWAN SSO has a copy of all plans.</p>		
16	System Interconnection / Information Sharing	<p>There was no evidence of Memoranda of Understanding (MOU), or Trading Partner Agreements (TPA), or that the internal interfaces had been addressed in the Security Plan.</p>		<p>Ensure all TIVWAN connections and information sharing with non-SFA entities are codified. See the section above on system interconnection and information sharing for further details.</p>		
17	Applicable Laws and Regulations	<p>TIVWAN is cognizant of applicable laws and regulations. The status of Privacy Act compliance is unknown. Although this system presumably complies with notice, publication, and annual/biennial/quadrennial review requirements, as those remain the responsibility of the Department's Chief Privacy Officer, no system-specific information with regard to access controls, storage, retrieval, retention, disclosure logging, contractor compliance, disposal of records, or employee training was provided for these systems.</p>		N/A		