File 20101001.0831: Notes on classified email 'major findings from I173'

Document title: 'Major Findings out of the CDTAB TRR for feedback to RM PMO'

(U) For RM 5.0 as standalone; no other capabilities were discussed; those will be discussed in follow-on TORAs.

(U) Tech Risk rating was High and 'follow-on capabilities will drive open the system's data risk'.

There were four issues:

- (U) rmuser account [details redacted]
- (U) MAC policy not implemented [details redacted]
- (U) not using resources on Solaris [details redacted]
- (U) remove root account after installation [details redacted]

Two new reports were published this week:

The first report was *Defense Intelligence Agency (DIA) Security Assessment Report (SAR) for Radiant Mercury Version 5.0 Baseline* dated 14 September 2010, S//NF [1].

details: DIA performed ST&E of RM 5.0 at USSTRATCOM, Western CONUS Regional Service Centre (WC RSC) Omaha, Nebraska 2–13 August 2010. It was the first operational installation of RM 5.0, and serves as both an operational and a Baseline ST&E event. It validated mitigations of findings from CT&E.

> (U) The purpose of the ST&E was to demonstrate that sufficient procedural and automated safeguards have been implemented within the system to permit the system to process the Top Secret information in an operational environment at Offutt AFB, Omaha, NE. Specifically, the objective of security certification testing is to show that Radiant Mercury operates with an acceptable level of risk as required by National and DoD standards. That is, to show that Radiant Mercury:
>
> a. satisfies operational requirements
> b. provides required user identification and authentication.
> c. provides required discretionary access control on files, application, and hosts.
> d. provides sufficient restrictions on access to security sensitive files.
> e. provides the capability to retrieve and display audit trail records.
> f. confirms that procedures for site backup, continuity of operations, and emergency destruction exist, if necessary.
> g. confirms that methods for site configuration management exist.

It notes that ST&E test procedures were originally created using DCID 6/3 requirements; following discussions amongst DIA, DNI, DoD, UCDMO and RM PMO, it was decided that RM 5.0 would instead go through the NIST C&A process instead of DCID 6/3. 'ST&E was followed by a comprehensive penetration test event by the DNI Certification, Accreditation and Test (CAT) Team.'

'The following recommendations have been provided:' [paraphrased]

- 'The Test Director recommends RM 5.0 be granted a Baseline Accreditation Letter.'
- and also receive an ATO with POA&M for STRATCOM for three years.

The next report to be issued this week, by the Office of the Director of National Intelligence, United States of America, was *System Assessment Test Report for Radiant Mercury (RM) System Version 5.0*, version 1.0, dated 2 September 2010, prepared by the IC CIO/ICIA CAT Team [2].

Summary: ODNI IC CIO Intelligence Community Information Assurance (ICIA) CAT Team performed penetration testing on the RM 5.0 system, in operational service at USSTRATCOM, WC RSC, Omaha, Nebraska from 16–20 August 2010. 'IC CIO/ICIA CAT Team was augmented by members of the STRATCOM Red Team, Dan Miller and AJ Newmaster,' whilst assessing Top Secret collateral and SIPRNet network infrastructures.

People notes: Corinne Catasnza is with IC CIO/ICIA CAT Team; she works for Calleen Torch, DNI/IC CIO/ICIA/CAT Chief.

References

[1] U. S. Defence Intelligence Agency. Defense Intelligence Agency (DIA) security assessment report (SAR) for Radiant Mercury version 5.0 Baseline, 14 September 2010. (S//NF).

[2] Office of the Director of National Intelligence, United States of America. System assessment test report for Radiant Mercury (RM) system version 5.0, 2 September 2010. Version 1.0, prepared by IC CIO/ICIA Certification, Accreditation and Test (CAT) Team, (S//NF).