

Information Technology Resource Management Council (ITRMC)

ENTERPRISE STANDARDS – S3000 NETWORK AND TELECOMMUNICATIONS

Category: S3120 – NETWORK SERVICES – DATA / NETWORK INTEGRITY

CONTENTS:

- I. [Definition](#)
- II. [Rationale](#)
- III. [Approved Standard\(s\)](#)
- IV. [Approved Product\(s\)](#)
- V. [Justification](#)
- VI. [Technical and Implementation Considerations](#)
- VII. [Review Cycle](#)
- VIII. [Time Line](#)
- IX. [Revision History](#)

I. DEFINITION

A data and network integrity system (DNI) is a system of hardware and software that compares data and file attributes to an established baseline and/or configuration policy. The DNI detects, logs and reports additions, deletions, or changes, and identifies affected systems and/or files. The DNI monitors the integrity of critical system files for both security (detection of attacks, collection of forensic evidence, etc.) and general system administration purposes.

II. RATIONALE

In digital government, both network availability and application/data integrity must be maintained in order to build a trusted infrastructure that fosters the confidence of citizens and system users. Data and network integrity verification is a security function that helps ensure this trusted infrastructure is maintained for the benefit of the entire enterprise. In addition, any data and network integrity solution must have an architecture that can be implemented within the enterprise security strategy and policy.

III. APPROVED STANDARD(S)

1. Secure Sockets Layer (SSL); and
2. Internet Protocol (IP).

IV. APPROVED PRODUCT(S)

1. Tripwire Manager;

2. Tripwire for Servers;
3. Tripwire for Web Pages; and
4. Tripwire for Routers and Switches.

V. JUSTIFICATION

Tripwire is recognized as the industry leader in data and network integrity products and technical expertise is available within the State to support this product. The Tripwire Manager's management console enables efficient management of Tripwire services across an enterprise network. Adoption of this standard will ease use and ensure compatibility for security services.

VI. TECHNICAL AND IMPLEMENTATION CONSIDERATIONS

The deployment, configuration and management of a data and network integrity system is a complex task requiring skilled resources.

VII. REVIEW CYCLE

Six (6) Months

VIII. TIME LINE

Last Reviewed: May 15, 2007
Last Revised: August 25, 2004
Effective Date: October 2, 2001

IX. REVISION HISTORY

8/25/04 – Revised rationale of standard for clarity.