(U//FOUO) New Policy: Preserving Intellectual Capital in the Event of a Disaster

FROM: [redacted]
Deputy Staff Chief, SIGINT Policy (S02L1)
Run Date: 09/15/2005

(U//FOUO) Are there *really* any plans in place for the continuity, recovery, and reconstitution of SIGINT mission and business functions in the event of a major emergency or disaster? Yes -- and all SID employees play a part!

(U//FOUO) The SIGINT Director recently signed SID Management Directive No. 412 , "Protection of United States SIGINT System Intellectual Capital Information," which **outlines the responsibilities of SID personnel for Intellectual Capital Recovery (ICR) in the event of an emergency or disaster.** All personnel working on SID activities shall have an obligation to identify and protect the Intellectual Capital (IC) for which they have responsibility. IC consists of:

- (U) mission applications source code information;
- (U) mission database information;
- (U) individually originated information;
- (U) operating system/Commercial-Off-The-Shelf (COTS) information;
- (U) mission policy, plans, processes, and procedures; and
- (U) legal and financial information.

This IC will be necessary to reestablish the SID mission in the event of a disaster affecting NSAW.

(C) The following guidance applies to ***all*** SID personnel: "All individually originated or maintained Intellectual Capital Information shall be stored routinely on the personal U:\drive (NT) or home directory (UNIX), or to group shared drives as appropriate."

(C) In addition, Directive 412 outlines special responsibilities for managers, records officers, program/project managers, system administrators, and the SIGINT Mission Assurance Systems Program Management Office.

(C//SI) After the events of September 11, 2001, the U.S. Government has been forced to assess various vulnerabilities facing SIGINT capabilities. The Mission Assurance program focuses on how to best sustain the SIGINT system's most critical operations and recover its capabilities in the event of a catastrophe.

(TS//SI) Accordingly, it is imperative that the single points of failure that exist within the current SID architecture are transitioned into a robust, geographically distributed, and inherently survivable architecture that can -- in the event of disaster -- support continuous delivery of mission-critical products and services to key customers. The strategy supporting this program includes standing up an alternate, remote, 24 hours a day -- 7 day a week operation, and load-sharing facility at [redacted] (an undisclosed location). In the event of a disaster at Fort Meade, this allows the continued ability to provide key intelligence to the National Command Authority.

(U//FOUO) Click on the below link to access this guidance:

SID Management Directive 412

(U//FOUO) The point of contact for this directive is [redacted] ([redacted]) of the Mission Assurance Project Management Office (PMO).

"(U//FOUO) SIDtoday articles may not be republished or reposted outside NSANet

without the consent of S0121 (DL sid_comms)."

DYNAMIC PAGE -- HIGHEST POSSIBLE CLASSIFICATION IS
TOP SECRET // SI / TK // REL TO USA AUS CAN GBR NZL
DERIVED FROM: NSA/CSSM 1-52, DATED 08 JAN 2007 DECLASSIFY ON: 20320108