CRYPTOME

16 September 2010

Source: CIA Freedom of Information Web Site: http://www.foia.cia.gov/

Inter-Agency Task Force on Unauthorized Disclosures Security Group

February 2, 2002

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Inter-Agency Task Force on Unauthorized Disclosures
Security Working Group

Tasking: The Interagency Task Force (IATF) on Unauthorized Disclosures Security Working Group was tasked with taking a fresh look at ways to organize and structure a more effective and comprehensive approach to addressing and minimizing the problem of unauthorized disclosures (leaks) of US classified intelligence information to the media. The purpose of this report is to provide the IATF with a brief overview of the Security Working Group's (SWG) progress to date.

Challenges

Number of Potential Suspects: The SWG members believe that measures to reduce the number of possible leak suspects would greatly assist in the task of identifying and sanctioning leakers. Even in cases in which highly sensitive restricted program information is leaked, investigators typically find that there are literally hundreds, if not thousands of individuals who had access to the compromised information. It is estimated that Intelink alone, has approximately 100,000 users. Today, increased collaboration requires even broader dissemination of classified information. The challenge, therefore, is identifying and deploying technical tools that will enhance the leaks investigator's ability to narrow the field of potential suspects.

Unified Effort: Another key area identified by the group is the need for a unified government-wide program to identify, analyze, and investigate media leaks and report investigative findings to appropriate officials for administrative or criminal sanctions. Currently, the various agencies of the Intelligence Community (IC) have their own agency-specific unauthorized disclosure programs. On virtually every media-leak related issue discussed, to include investigative tools, processes and policies, the group found little uniformity. For a variety of reasons, many organizations lack formal dedicated media leak investigation programs. With some exceptions, in the past 10 years, the only individuals who have been identified and administratively sanctioned for leaking classified information to the media were those who self-confessed or were identified by the media as the source of the leaked information. The group believes that a more unified IC, OGA, and Industry wide program, including establishment of leak detection units in each agency and a community-wide leaks investigation unit, would significantly enhance the identification, authentication, investigation and prosecution of media leaks.

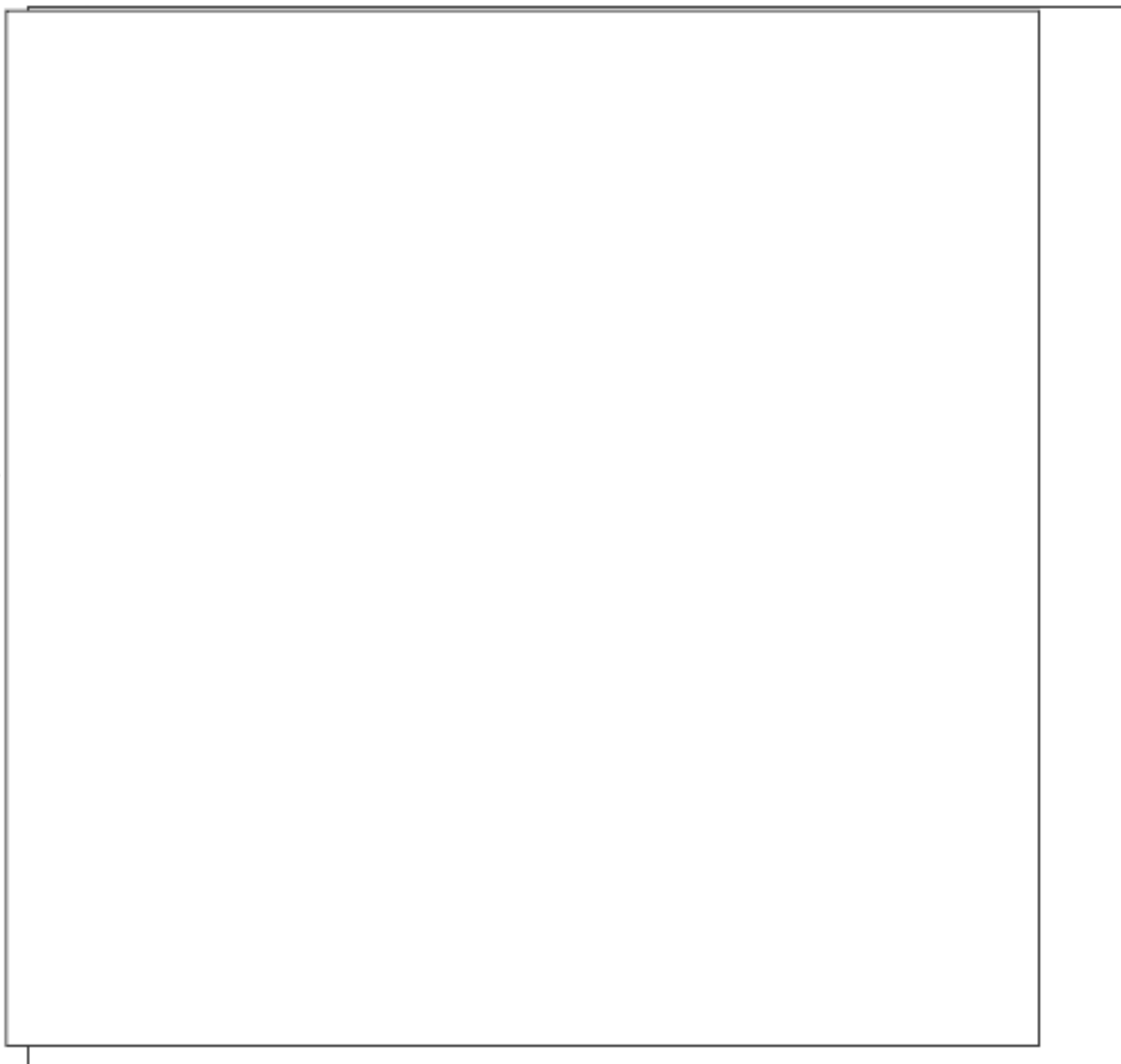ALL PORTIONS UNCLASSIFIED//FOR OFFICIAL USE ONLY

(100)

Lessons Learned

Past attempts to coordinate the Community have met with only sporadic and minimal results. The DCI's Unauthorized Disclosure Analysis Center (1986-1992) (UDAC) incorporated some Intelligence Community participation and an analytical arm, but lacked investigative and education capabilities. As a result, media leak analysis and leak investigations were almost totally disconnected and uncoordinated.

Recommendation:

SECURITY WORKING GROUP ISSUES

1. What sanctions have been imposed on government employees in the past 5-10 years for leaks; for mishandling classified information?

2. Warrantless Searches of US Government offices:

   — DOJ policy imposed government-wide

   — Adverse inference in Administration Proceeding

3. Single Issue Polygraphs:

   — Adverse Inference in Administration Proceeding

4. Refusal to answer questions or be interviewed:

   — Adverse inference in Administrative proceeding

5. DCI is statutorily required to protect sources and methods of intelligence:

   — Is he applying adequate resources to this endeavor?

6. Traps and traces on government phones:

   — cost
   — feasibility

7. Develop educational programs:

   — What programs are currently in place?
   — remark on their efficacy utility

OPR 63