b7E

4.6.2. (U) Release of Information to U.S. Government Entities

(U//FOUO) CyD and FOs are often in the position of sharing information with other USG entities to further intelligence gathering and operational interests. After conducting an equity review, CyD and FOs are encouraged to share information if it is in the best interest of the FBI.

(U//FOUO) The sharing of classified and unclassified information with a USG member must be initiated with an EC, which must have an accompanying letterhead memorandum (LHM). The EC may be drafted by CyD or an FO and must be approved by the appropriate CyD substantive desk UC. The dissemination of information to USG members must also be documented in an FD-999, "Liaison With External Organizations" (see DIOG subsection 12.6).

b7E

4.7. (U) Victim Notification in Computer Intrusion Matters

(U//FOUO) CyD's top priority is the protection of our national security, economy, and information infrastructure from intrusions, malicious code, and nefarious computer network operations. This effort entails the sharing of investigative information with intrusion victims and the CND community to protect compromised systems, mitigate economic loss and damage, and prevent future attacks. Victim notification is a compelling way for CyD to contribute to network defense for the protection of individual, commercial, and government users of the Internet, as well as for the protection of the infrastructure itself. It is the policy of CyD to notify and disseminate meaningful information to victims and the CND community in a timely manner to the extent to which it does not interfere with ongoing law enforcement or USIC investigations, operations, methods, sources, or technologies.

(U//FOUO) In a computer intrusion investigation, the victim to be notified is the individual, organization, or corporation that is the owner or operator of the computer at the point of compromise or intrusion. Cyber victims are generally individuals or organizations subjected to cyber-based operations, including computer network attack (CNA) and computer network exploitation (CNE), in furtherance of criminal activity or threats to national security. These CNA and CNE operations often result in the compromise of electronic systems, resulting in the alteration, loss, exfiltration, or denial of access to data that the victim maintains or controls. Victims may be identified, to the extent possible, by the FBI or its partner agencies in the course of investigative activities of suspected cybercrimes and cyber-related threats.

b7E

b7E

(U//FOUO) Because timely victim notification has the potential to completely mitigate ongoing and future intrusions and can mitigate the damage of past attacks while increasing the potential for the collection of actionable intelligence, CyD's policy regarding victim notification is designed to strongly favor victim notification. Even when it may interfere with another investigation or USIC operation, notification should still be considered in coordination with the operational stakeholders when the equities of victim notification serve to protect USPERs, a national infrastructure, or other U.S. interests from significant harm.

4.7.1. (U) Victim Notification Test

(U//FOUO) The Attorney General (AG) has issued guidelines that create a mandatory victim notification paradigm which requires, under certain circumstances, that federal investigators and prosecutors identify victims of crime and, among other required actions, notify them of the crime, except where the notification would interfere with an ongoing investigation (see the *Attorney General Guidelines for Victim and Witness Assistance*, Article IV).

b7E

(U//FOUO) To ensure that decisions relating to providing notice to a victim in a cyber investigation are consistent, the following analysis must be conducted prior to providing notice to a victim:

b7E

b7E

4.7.2. (U) Approval or Deferral of Notification

b7E

b7E

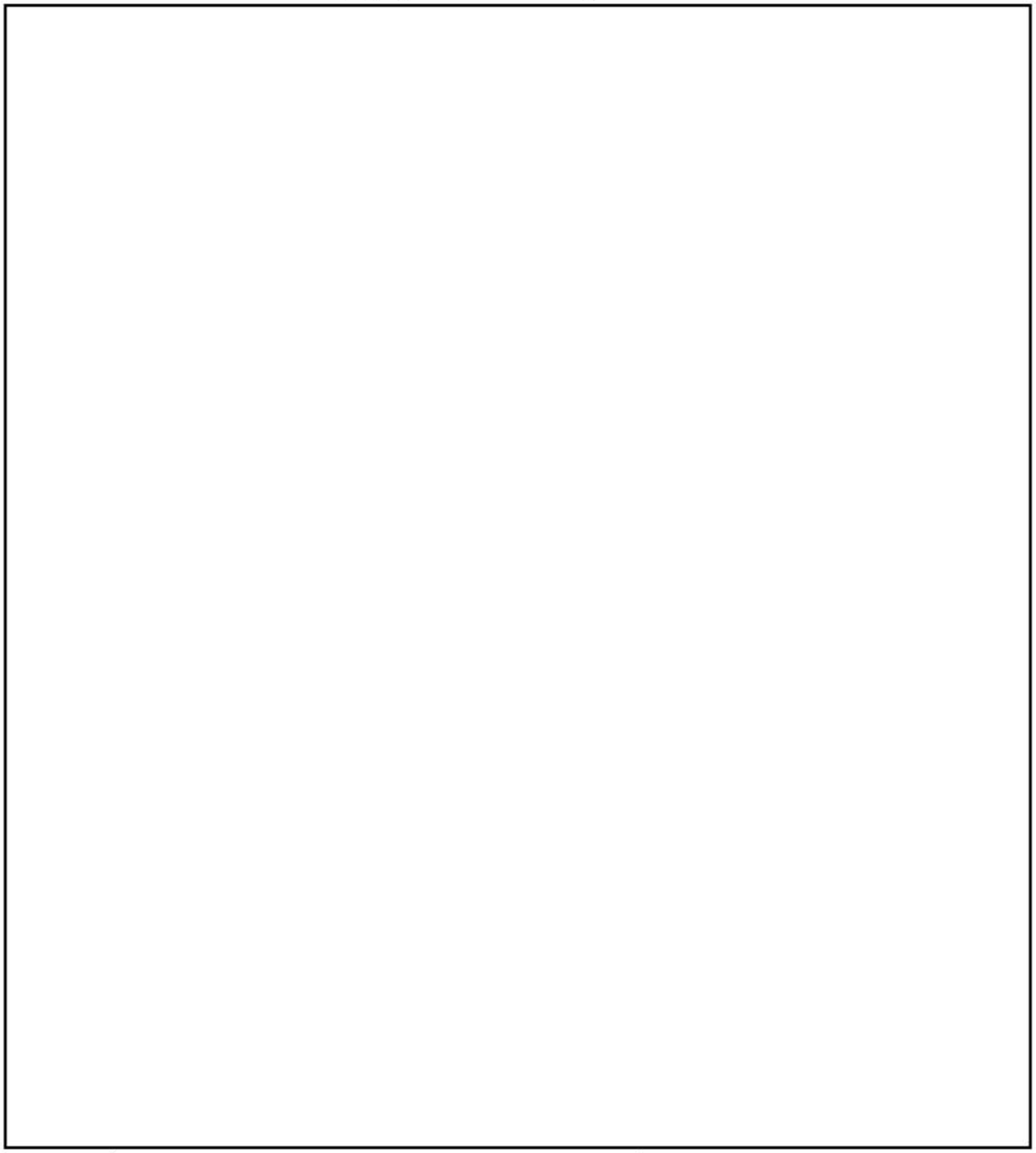
4.7.3. (U) Timing of Notification

b7E

4.7.4. (U) Method of Notification

b7E

b7E



4.7.5.

b7E

b7E

4.8. (U) Claiming Statistical Accomplishments

(U//FOUO) In evaluating the FBI's overall performance and accountability, disruption and dismantlement (D&D) statistics are routinely disseminated to the DOJ, the Office of Management and Budget (OMB), and the General Accounting Office (GAO). These statistics assist in determining the overall effectiveness of the FBI's ability to combat criminal threats. Furthermore, these statistics are included in Congressional budget submissions in order to meet the requirements of the Government Performance and Results Act (GPRA).

(U//FOUO) Therefore, to ensure accuracy and consistency in claiming D&D accomplishments, any division or FO requesting to claim a D&D accomplishment must first obtain approval of the UC of the responsible TU. This may be accomplished by routing the document through the claimant's squad supervisor as the first approver and then selecting the UC role of the substantive TU as the final accomplishment approver.

4.9. (U) Cyber Training and Logistics

(U) The Cyber Training and Logistics Unit (CTLU) is responsible for monitoring the technical competency of all employees assigned to support the cyber mission. The unit assesses the competency of the cyber workforce and strategically develops and delivers mission-related training to maximize the limited financial resources allocated to the development of the workforce. The workforce includes, but is not limited to, SAs, SSAs, IAs, and TFOs assigned to cyber investigations, as well as professional staff working within CyD.

4.9.1. (U) Cyber Special Agent Career Path Developmental Plan

(U) The cyber SA career path developmental plan sets forth the recommended required and elective training courses and experiential milestones for each stage of the career path. The courses integrated into this plan are intended to provide investigators with the skills needed to successfully work cases in support of CyD priorities; the plan also includes a series of elective courses that allow investigators to explore and develop expertise with specific OSs and technologies. Appropriate development options are identified in a training map posted on the CTLU Intranet site.

4.9.2. (U) Test-Out Options for Investigators With Technical Expertise

(U) Many of the training classes offered by CTLU are technical in nature. Recognizing that personnel working cyber matters bring varying levels of technical expertise with them to the