Appendix B
Best Practices for Working with Companies

Intrusion crimes can damage or impair the functioning of computers and networks. Victims may be the intended targets of the intrusion or third parties whose systems are used to carry out unlawful activity, such as universities and Internet service providers. After a company reports an intrusion, there are a number of "best practices" for law enforcement that can make the relationship between law enforcement and companies more productive in the aftermath of a computer incident. The practices discussed here are designed to be implemented in addition to, not in lieu of, the Attorney General Guidelines for Victim and Witness Assistance.[1] Also, please note that the Secret Service publishes a guide on the mechanics of seizing computer evidence, *Best Practices for Seizing Electronic Evidence, available at* http://www.forwardedge2.com/pdf/bestPractices.pdf.

Because computer information systems are essential to the everyday operation of most businesses, the disruption of those services can cripple a company. Law enforcement should remain aware of the tension between their need to collect evidence for prosecution and the company's need to resume operations as quickly as possible. Also, companies usually wish to avoid the negative publicity frequently associated with a breach of network security.

Because victims play an important role in providing computer logs and factual testimony regarding the intrusion, we also suggest some "best practices" for companies to consider when responding to a network crime. These suggested practices are in Appendix C.

In general, law enforcement should seek to build a trusted relationship with companies. Keeping these goals in mind will help to obtain timely assistance from companies and increase the likelihood of successful prosecutions.

[1] The current copy of the Attorney General Guidelines for Victim and Witness Assistance can found at: http://www.ojp.usdoj.gov/ovc/publications/welcome.html.

1. Protect the Rights of the Victim

Law enforcement should ensure that the victim's rights under 18 U.S.C. § 3771(a) are honored, including the rights to

- reasonable protection from the accused
- accurate and timely notice of court proceedings involving the crime or of any release or escape of the accused
- not be excluded from any such public court proceeding, unless the court determines that testimony by the victim would be materially altered if the victim heard other testimony at that proceeding
- be heard at any public proceeding in the district court involving release, plea, sentencing, or probation
- confer with the government attorney on the case
- full and timely restitution as provided in law
- proceedings free from unreasonable delay
- be treated with fairness and with respect for the victim's dignity and privacy

2. Consult with Senior Management

Consulting with the company's senior management before undertaking investigative measures on the company's network will often pay dividends. Some decisions require the authorization of a company's senior management. For example, system administrators may lack authority to consent to law enforcement activities that will affect business operations. In addition, be aware that if the company or its employees are represented by legal counsel in the matter, direct contact with those persons may be restricted absent the attorney's consent. This ethical constraint binds Department of Justice attorneys as well as the agents operating on their behalf.

3. Consult with Information Technology Staff

Whenever possible, we suggest consulting with the company's information technology staff about network architecture before implementing investigative measures on the network. Working closely with the information technology staff will help to obtain important information, including information regarding network topology. Helpful information will include the type and version of software being run on the network and any peculiarities in the architecture of the network, such as proprietary hardware or software. Obtaining this information will help to ensure that law enforcement can obtain all information relevant

to an investigation and minimize disruption of the company's network from investigative measures.

Specific things to identify in a network include the locations of intrusion detection systems, network switches, and firewalls. Also, identify all data logs, including the type data being logged, the size of the log files (to check for losing data due to rolling retention), and location of the logs (sent to a log server or maintained on the hacked system and subject to compromise themselves).

4. Minimize Disruption to the Company

Law enforcement should make every effort to use investigative measures that minimize computer downtime and displacement of a company's employees. Some investigative measures are indispensable despite the inconvenience to a company. Other investigative steps may be altered or avoided if they needlessly aggravate employees or prolong the damage already suffered by a company. For example, rather than seizing compromised computers and depriving the company of their use, consider creating a "mirror image" of the system and leaving computers in place. Also, consider practical issues such as whether raid jackets or other insignia are appropriate to display.

Similarly, although consulting with company system administrators and computer experts is essential, avoiding excessive burdens on these personnel can help promote the trust and goodwill of company.

5. Coordinate Media Releases

Investigations and prosecutions of cybercrime cases may entail the release of information by law enforcement in press releases or press conferences. All press releases and press conferences should be coordinated with the Office of Public Affairs at (202) 514-2007.

Additionally, public statements to the news media should also be coordinated with the company to ensure that these statements do not needlessly reveal information harmful to a company. Informing companies of this coordination at an early stage in the investigation is an important step. Fear of damage to carefully built reputations is a major reason why companies refrain from reporting crime to law enforcement. Law enforcement should take all possible

measures to prevent unauthorized releases of information about pending investigations and to punish unauthorized disclosures when they occur.

In return, consider asking the company to allow the investigating agents to review any press releases regarding the investigation before issuing them. This will prevent the company from releasing information that could damage the investigation.

6. Keep the Company Informed About the Investigation

After conducting the initial on-site investigation, law enforcement may have little direct contact with a company. To the extent possible—recognizing the need to guard against disclosure of grand jury information or information that could otherwise jeopardize the investigation—keep the company informed of the progress of the investigation. In addition, where an arrest is made that results in court proceedings, notify the company of all significant court dates so company personnel have the opportunity to attend.

7. Build Relationships Before an Intrusion

Many companies, universities, and other victims are reluctant to report cybercrime incidents to law enforcement because they are fearful that law enforcement will conduct an investigation in a manner harmful to their operational interests or because they have misconceptions about how law enforcement will conduct an investigation. Such fears and misconceptions can more easily be dispelled if law enforcement has a pre-existing relationship with a company, rather than having the company's first contact with law enforcement come in the midst of a crisis. For example, forming liaison groups comprised of law enforcement and private industry representatives can help bridge gaps of mistrust or unfamiliarity and increase future cybercrime reporting by private industry.