CIO CYBERTHREAT RESPONSE & REPORTING GUIDELINES

COMPONENTS

- Background and Scope of Project
- CIO Cyberthreat Response & Reporting Guidelines
- Who to Contact: Law Enforcement
- Who to Contact: Reporting Bodies & Resources for Cyberthreat Response
- FBI and USSS Field Office contact list
- Report Form—short, standard, first-alert form
- Contributors

CIO CYBERTHREAT RESPONSE & REPORTING PROJECT

A collaboration among industry professionals, law enforcement and CIO *Magazine to develop guidelines for reporting computer security incidents to law enforcement*

At the CIO Perspectives conference in Palm Springs in October 2001, audience members (chief information officers and other executives) were encouraged by the U.S. Attorney for Los Angeles to report cybersecurity breaches to law enforcement as part of the war against terrorism. But, as one CIO asked: "We get hit thousands of times a month; do you want us to report all of these incidents? And exactly who do we contact?" Other audience members expressed similar bewilderment, and that's what prompted this initiative.

Goal This project has a modest goal: to provide a basic understanding of what is required for cyberthreat incident response and to make it as easy as possible to report such incidents to law enforcement (including whom to call and what to tell them). For this effort, we restricted our recommendations to reporting incidents that are an attack on information systems or data (computer and/or Internet security). We did not attempt to address other types of cybercrime such as Internet fraud or pornography.

A Complex Issue Creating and maintaining a secure information environment is difficult, expensive and complicated. Risk assessment; control selection and deployment; monitoring/detection; incident response and continuous improvement must all be considered together. Prevention is, of course, the primary objective.

Incident response is itself a complex subject, including the sometimes difficult decision of whether to share any information at all. There are many excellent resources available to help CIOs and CISOs (chief information security officers) understand and address these challenges; you'll find some of them listed at the end of this document under "Resources."

Why You Should Report Cybercrime Only by sharing information with law enforcement and appropriate industry groups will we be able to identify and prosecute cybercriminals, identify new cybersecurity threats and prevent successful attacks on our critical infrastructures and economy. Law enforcement's ability to identify coordinated threats is directly tied to the amount of reporting that takes place.

We understand that you might be reluctant to share information regarding the impact to your business and the sensitivity of the data involved. While we will not make the case here for trusting various agencies or organizations, we encourage you to learn more about how law enforcement and other reporting bodies approach these issues in terms of the likely impact of their investigation on your business and how they handle sensitive information.

CIO CYBERTHREAT RESPONSE & REPORTING GUIDELINES

An organization must respond in some way to a computer security breach—whether it is an intrusion/hack, the implantation of malicious code such as a virus or worm, or a denial of service attack. The better prepared the organization is to respond quickly and effectively, the better chance it will have to minimize the damage. These guidelines are intended to provide a framework and starting point for developing a cyberthreat response and reporting capability.

PLANNING

- Develop an incident response plan and designate people to carry it out. The plan should include details for how you will:
  - detect the incident
  - analyze the incident
  - contain or eradicate the problem
  - provide workarounds or fixes
  - prevent re-infection
  - log events
  - preserve evidence
  - conduct a post-mortem and apply lessons learned
- Educate users to raise security awareness and promote security policies.
- Build a centralized incident reporting system.
- Establish escalation procedures that lay out actions the company should take if an attack turns out to be protracted or especially damaging.
- Make sure your service-level agreements include provisions for security compliance, and spell out reporting requirements and maintenance of systems (including contingency plans) in the event of a cyberattack.
- Decide in advance under what circumstances you'd call the authorities.
- Plan how and when employees, customers and strategic partners will be informed of the problem.
- Establish communication procedures should this become a media event.

PEOPLE

- Have a single contact to whom employees should report suspicious events and who will track changes in contacts or procedures.
- Have a single contact who will report incidents to outside agencies, including law enforcement, regulatory bodies and information sharing organizations such as InfraGard and the industry Information Sharing and Analysis Centers (ISACs).
- Keep a list of the incident response team members' names, titles and 24/7 contact information, along with their role in a security breach.
- Have contact information for vendors contracted to help during a security emergency, as well as ISPs and other relevant technology providers.
- Have contact information for major customers and clients who might be affected.
- In advance, establish contacts at the relevant law-enforcement agencies: typically, the national infrastructure protection and computer intrusion squad at the local FBI field office; the electronic crimes investigator at the local Secret Service field office; and the electronic crimes investigator at your local police. Have their contact information easily accessible.

PROCESS

- Perform a risk analysis on your plan.
- Test/rehearse procedures periodically.
- Develop contingency plans in case your response infrastructure is attacked.

WHAT TO REPORT

You should report cybersecurity events that have a real impact on your organization (when damage is done, access is achieved by the intruder, loss occurs, malicious code is implanted) or when you detect something noteworthy or unusual (new traffic pattern, new type of malicious code, specific IP as source of persistent attacks).

At this time, we do not recommend that you report routine probes, port scans or other common events. Neither law enforcement nor the ISACs are prepared to receive or analyze the enormous volume of data this would entail. While such detailed "hit" data has potential value in identifying and defining trends, and facilities like the Internet Storm Center (at the SANS Institute) or the NIPC may eventually get set up to collect detailed event logs, right now it is generally not useful.

Consequently, the form we recommend is designed to report significant, unusual or noteworthy incidents.

WHEN AND HOW TO REPORT AN INCIDENT

If an attack is under way, you'll want to pick up the phone and call your previously established law-enforcement contact immediately and communicate the

basic information that is included in the CIO Cyberthreat Response Form. There is additional information that will be required to effectively conduct the investigation (see bullet points below), but the form is a good place to start.

Sometimes you will report an incident to law enforcement after the fact—you have detected that something happened, but your systems are functioning normally and whatever damage is likely has already been done. In this case, you will want to gather as much information as possible for the law enforcement agents before you make the call.

Here is some additional information that will help law enforcement agents in their investigation:

- What are the primary systems involved?
- How was the attack carried out?
- What steps have you taken to mitigate or remediate?
- Does a suspect exist? If so, is it a current or former employee/contractor?
- What evidence is available to assist in the investigation (e.g., log files, physical evidence, etc.?)

To track the status of your case once you've filed a report, contact the field office that is conducting the investigation.

WHO TO CONTACT

LAW ENFORCEMENT

There is no single answer for which law enforcement agency to contact in the event of a cyber-security breach. The FBI and U.S. Secret Service share jurisdiction for computer crimes that cross state lines. However, most law enforcement agencies, including the FBI and USSS, encourage people to a) preestablish contact with someone in law enforcement who is trained in and responsible for dealing with computer crime, and b) work with the person or people you have the best relationship with, regardless of agency.

FEDERAL AGENCIES, LOCAL CONTACTS

FBI Field Office Call the national infrastructure protection and computer intrusion squad at the local field office.*

U.S. Secret Service Field Office Contact the electronic crimes investigator at the local field office.*

*A list of local field offices follows Page 6.

FEDERAL AGENCIES, WASHINGTON

FBI/National Infrastructure Protection Center (NIPC)
J. Edgar Hoover Building
935 Pennsylvania Avenue, NW
Washington, DC 20535-0001
phone: (202) 323-3205; 888-585-9078
fax: (202) 323-2079
e-mail: *nipc.watch@fbi.gov*
website: *www.nipc.gov*
reporting: *www.nipc.gov/incident/cirr.htm*

Electronic Crimes Branch of the U.S. Secret Service Headquarters
950 H Street, NW
Washington, DC 20223
phone: (202) 406-5850
fax: (202) 406-5031
website & reporting: *www.treas.gov/usss*

STATE & LOCAL AGENCIES

State Attorney General's Office The website for the National Attorney Generals' Association provides a list with contact information by state.
www.naag.org/issues/20010724-cc_list.cfm

Local Police: The CrisNet website offers a list of local law enforcement agencies organized by state.
www.crisnet.com/locallaw/locallaw.html

OTHER REPORTING BODIES & RESOURCES FOR CYBERTHREAT SUPPORT

Most of the following organizations not only serve as coordination points for reporting incidents, but they also offer lots of useful information for network security and incident response.

National Infrastructure Protection Center (NIPC)
Focal point for threat assessment, warning, investigation and response for threats or attacks against United States critical infrastructures.
www.nipc.gov

InfraGard
Public/private information-sharing effort led by the FBI and the NIPC. Local chapters across the United States. Great place to develop appropriate contacts with law enforcement.
www.infragard.net

Electronic Crimes Task Force
Public/private info-sharing effort led by the U.S. Secret Service. Regional task forces located across the United States, and a great place to develop computer-crime law-enforcement contacts.
www.ectaskforce.org/Regional_Locations.htm

Information Sharing & Analysis Centers (ISACs)
Industry specific information sharing for critical infrastructure sectors.
For general information on the ISACs, see https://www.it-isac.org/isacinfowhtppr.php

Electric . . . . . .*www.nerc.com*
Financial Services . . .*www.fsisac.com*
IT . . . . . .*www.it-isac.org*
Oil & Gas . . . . . .*www.energyisac.com*
Telecom . . . . . .*www.ncs.gov & www.ncs.gov/Image-Files/ISAC_Fact.pdf*
U.S Govt. . . . . .*www.fedcirc.gov*
Water . . . . . .*www.amwa.net/isac/*

Forum of Incident Response and Security Teams
A network of computer security incident response teams and info sharing designed for the private sector.
www.first.org

Department of Justice Computer Crime & Intellectual Property Section
Legal analysis and resources related to computer crime, a how-to-report section and a comprehensive list of cybercrime cases pending and resolved.
www.cybercrime.gov

CERT Coordination Center at Carnegie Mellon
Federally funded research center provides training, incident handling, R&D, advisories. Lots of good information resources available to the public.
www.cert.org

SANS Institute
Cooperative research organization offers alerts, training and certification; operates Incidents.org and the Internet Storm Center. Like CERT, has lots of good information resources on its website.
www.sans.org
www.incidents.org

ADDITIONAL RESOURCES

***CIO* Magazine Security and Privacy Research Center**
A collection of articles, guidelines and links for information security issues from an executive perspective.
www.cio.com/research/security

Specific Documents
Practices for Protecting Information Resources Assets
Texas Dept. of Information Resources
www.dir.state.tx.us/IRAPC/practices/index.html

Handbook for Computer Security Incident Response Teams
Carnegie Mellon University
www.sei.cmu.edu/pub/documents/98.reports/pdf/98hb001.pdf

Minimizing Your Potential Vulnerability and Enhancing Effective Response
NIPC
www.nipc.gov/incident/incident3.htm

Sample Incident Handling Procedure
www.csirt.ws/docs/incident.handling.pro.doc

Best Practices for Seizing Electronic Evidence
A Joint Project of the International Association of Chiefs of Police and the U.S. Secret Service
www.treas.gov/usss/electronic_evidence.htm

FBI & USSS FIELD OFFICES

TELEPHONE/FAX
ADDRESS

ALABAMA

Birmingham
FBI 205.326.6166/205.715.0232
2121 8th Avenue N.
Birmingham, AL 35203-2396
USSS 205.731.1144/205.731.0007
Daniel Building
15 South 20th Street, Suite 1125
Birmingham, AL 35233

Mobile
FBI 334.438.3674/251.415.3235
One St. Louis Centre
1 St. Louis Street, 3rd Floor
Mobile, AL 36602-3930
USSS 334.441.5851/334.441.5250
Parkview Office Building
182 St. Francis Street
Mobile, AL 36602

Montgomery
USSS 334.223.7601/334.223.7523
Colonial Financial Center
1 Commerce Street, Suite 605
Montgomery, AL 36104

ALASKA

Anchorage
FBI 907.276.4441/907.265.9599
101 East Sixth Avenue
Anchorage, AK 99501-2524
USSS 907.271.5148/907.271.3727
Federal Building & U.S. Courthouse
222 West 7th Avenue, Room 559
Anchorage, AK 99513

ARIZONA

Phoenix
FBI 602.279.5511/602.650.3024
201 East Indianola Avenue, Suite 400
Phoenix, AZ 85012-2080
USSS 602.640.5580/602.640.5505
3200 North Central Avenue, Suite 1450
Phoenix, AZ 85012

Tucson
USSS 520.670.4730/520.670.4826
300 West Congress Street, Room 4-V
Tucson, AZ 85701

ARKANSAS

Little Rock
FBI 501.221.9100/501.228.8509
24 Shackleford West Boulevard
Little Rock, AR 72211-3755
USSS 501.324.6241/501.324.6097
111 Center Street, Suite 1700
Little Rock, AR 72201-4419

CALIFORNIA

Fresno
USSS 209.487.5204/559.487.5013
5200 North Palm Avenue, Suite 207
Fresno, CA 93704

Los Angeles
FBI 310.477.6565/310.996.3359
Federal Office Building
11000 Wilshire Boulevard, Suite 1700
Los Angeles, CA 90024-3672
USSS 213.894.4830 213.894.2948
Roybal Federal Building
255 East Temple Street, 17th Floor
Los Angeles, CA 90012

Riverside
USSS 909.276.6781/909.276.6637
4371 Latham Street, Suite 203
Riverside, CA 92501

Sacramento
FBI 916.481.9110/916.977.2300
4500 Orange Grove Avenue
Sacramento, CA 95841-4205
USSS 916.930.2130/916.930.2140
501 I Street, Suite 9500
Sacramento, CA 95814-2322

San Diego
FBI 858.565.1255/858.499.7991
Federal Office Building
9797 Aero Drive
San Diego, CA 92123-1800
USSS 619.557.5640/619.557.6658
550 West C Street, Suite 660
San Diego, CA 92101

San Francisco
FBI 415.553.7400/415.553.7674
450 Golden Gate Avenue, 13th Floor
San Francisco, CA 94102-9523
USSS 415.744.9026/415.744.9051
345 Spear Street
San Francisco, CA 94105

San Jose
USSS 408.535.5288/408.535.5292
U.S. Courthouse & Federal Building
280 S. First Street, Suite 2050
San Jose, CA 95113

Santa Ana
USSS 714.246.8257/714.246.8261
200 W. Santa Ana Boulevard,
Suite 500
Santa Ana, CA 92701-4164

Ventura
USSS 805.339.9180/805.339.0015
5500 Telegraph Road, Suite 161
Ventura, CA 93003

COLORADO

Colorado Springs
USSS 719.632.3325/719.632.3341
212 N. Wahsatch, Room 204
Colorado Springs, CO 80903

Denver
FBI 303.629.7171/303.628.3085
1961 Stout Street, 18th Floor
Denver, CO 80294-1823
USSS 303.866.1010/303.866.1934
1660 Lincoln Street
Denver, CO 80264

CONNECTICUT

New Haven
FBI 203.777.6311/203.503.5098
600 State Street
New Haven, CT 06511-6505
USSS 203.865.2449/203.865.2525
265 Church Street, Suite 1201
New Haven, CT 06510

DELAWARE

Wilmington
USSS 302.573.6188/302.573.6190
One Rodney Square
920 King Street, Suite 414
Wilmington, DE 19801

DISTRICT OF COLUMBIA

Washington, D.C.
FBI (HDQRS.)
202.278.2000/202.278.2478
601 4th Street NW
Washington, D.C. 20535-0002
USSS 202.406.8000/202.406.8803
1100 L Street NW, Suite 6000
Washington, D.C. 20005
USSS (HDQRS.)
202.406.5850/202.406.5031
950 H Street NW
Washington, D.C. 20223

FLORIDA

Jacksonville
FBI 904.721.1211/904.727.6242
7820 Arlington Expressway
Jacksonville, FL 32211-7499
USSS 904.296.0133/904.296.0188
7820 Arlington Expressway,
Suite 500
Jacksonville, FL 32211

Miami
FBI 305.944.9101/305.787.6538
16320 NW Second Avenue
North Miami Beach, FL 33169-6508
USSS 305.629.1800/305.629.1830
8375 NW 53rd Street
Miami, FL 33166

Orlando
USSS 407.648.6333/407.648.6606
135 West Central Boulevard,
Suite 670
Orlando, FL 32801

Tallahassee
USSS 850.942.9523/850.942.9526
Building F
325 John Knox Road
Tallahassee, FL 32303

Tampa
FBI 813.273.4566/813.272.8019
Federal Office Building
500 Zack Street, Room 610
Tampa, FL 33602-3917
USSS 813.228.2636/813.228.2618
501 East Polk Street, Room 1101
Tampa, FL 33602

West Palm Beach
USSS 561.659.0184/561.655.8484
505 South Flagler Drive
West Palm Beach, FL 33401

GEORGIA

Albany
USSS 229.430.8442/229.430.8441
Albany Tower
235 Roosevelt Avenue, Suite 221
Albany, GA 31702

Atlanta
FBI 404.679.9000/404.679.6289
2635 Century Parkway Northeast,
Suite 400
Atlanta, GA 30345-3112
USSS 404.331.6111/404.331.5058
401 West Peachtree Street, Suite 2906
Atlanta, GA 31702

Savannah
USSS 912.652.4401/912.652.4062
33 Bull Street
Savannah, GA 31401

HAWAII

Honolulu
FBI 808.566.4300/808.566.4470
Kalanianaole Federal Office Building
300 Ala Moana Boulevard, Room 4-230
Honolulu, HI 96850-0053
USSS 808.541.1912/808.545.4490
Kalanianaole Federal Office Building
300 Ala Moana Boulevard, Room 6-210
Honolulu, HI 96850

IDAHO

Boise
USSS 208.334.1403/208.334.1289
Federal Building – U.S. Courthouse
550 West Fort Street, Room 730
Boise, ID 83724-0001

ILLINOIS

Chicago
FBI 312.421.4310/312.786.2525
E.M. Dirksen Federal Office Building
219 South Dearborn Street, Room 905
Chicago, IL 60604-1702
USSS 312.353.5431/312.353.1225
Gateway IV Building
300 S. Riverside Plaza, Suite 1200 North
Chicago, IL 60606

Springfield
FBI 217.522.9675/217.535.4440
400 West Monroe Street, Suite 400
Springfield, IL 62704-1800
USSS 217.492.4033/217.492.4680
400 West Monroe Street, Suite 301
Springfield, IL 62704

FBI & USSS FIELD OFFICES

TELEPHONE/FAX
ADDRESS

INDIANA
Evansville
USSS 812.985.9502/812.985.9504
P.O. Box 530
Newburgh, IN 47630
Indianapolis
FBI 317.639.3301/317.321.6193
Federal Office Building
575 N. Pennsylvania Street,
Room 679
Indianapolis, IN 46204-1585
USSS 317.226.6444/317.226.5494
Federal Office Building
575 N. Pennsylvania Street,
Suite 211
Indianapolis, IN 46204-1585
South Bend
USSS 219.273.3140/219.271.9301
P.O. Box 477
South Bend, IN 46625

IOWA
Des Moines
USSS 515.284.4565/515.284.4566
210 Walnut Street, Suite 637
Des Moines, IA 50309-2107

KANSAS
Wichita
USSS 316.269.6694/316.269.6154
Epic Center
301 N. Main Street, Suite 275
Wichita, KS 67202

KENTUCKY
Lexington
USSS 859.223.2358/859.223.1819
3141 Beaumont Centre Circle
Lexington, KY 40513
Louisville
FBI 502.583.3941/502.569.3869
Federal Building
600 Martin Luther King Jr. Place,
Room 500
Louisville, KY 40202-2231
USSS 502.582.5171/502.582.6329
Federal Building
600 Martin Luther King Jr. Place,
Room 377
Louisville, KY 40202-2231

LOUISIANA
Baton Rouge
USSS 225.389.0763/225.389.0325
One American Place, Suite 1502
Baton Rouge, LA 70825
New Orleans
FBI 504.816.3000/504.816.3306
2901 Leon C. Simon Drive
New Orleans, LA 70126
USSS 504.589.4041/504.589.6013
Hale Boggs Federal Building
501 Magazine Street
New Orleans, LA 70130
Shreveport
USSS 318.676.3500/318.676.3502
401 Edwards Street
Shreveport, LA 71101

MAINE
Portland
USSS 207.780.3493/207.780.3301
100 Middle Street
West Tower, 2nd Floor
Portland, ME 04101

MARYLAND
Baltimore
FBI 410.265.8080/410.281.0339
7142 Ambassador Road
Baltimore, MD 21244-2754
USSS 410.962.2200/410.962.0840
100 S. Charles Street, 11th Floor
Baltimore, MD 21201
Eastern Shore
USSS 410.268.7286/410.268.7903
U.S. Naval Academy
Police Dept., Headquarters Building 257,
Room 221
Annapolis, MD 21402
Frederick
USSS 301.293.6434/301.694.8078
Rowley Training Center
9200 Powder Mill Road, Route 2
Laurel, MD 20708

MASSACHUSETTS
Boston
FBI 617.742.5533/617.223.6327
One Center Plaza, Suite 600
Boston, MA 02108
USSS 617.565.5640/617.565.5659
Thomas P. O'Neill Jr. Federal Building
10 Causeway Street
Boston, MA 02222

MICHIGAN
Detroit
FBI 313.965.2323/313.237.4009
Patrick V. McNamara Building
477 Michigan Avenue, 26th Floor
Detroit, MI 48226
USSS 313.226.6400/313.226.3952
Patrick V. McNamara Building
477 Michigan Avenue
Detroit, MI 48226
Grand Rapids
USSS 616.454.4671/616.454.5816
330 Ionia Avenue NW, Suite 302
Grand Rapids, MI 490503-2350
Saginaw
USSS 989.752.8076/989.752.8048
301 E. Genesee, Suite 200
Saginaw, MI 48607

MINNESOTA
Minneapolis
FBI 612.376.3200/612.376.3249
111 Washington Avenue South,
Suite 1100
Minneapolis, MN 55401-2176
USSS 612.348.1800/612.348.1807
U.S. Courthouse
300 South 4th Street, Suite 750
Minneapolis, MN 55415

MISSISSIPPI
Jackson
FBI 601.948.5000/601.360.7550
Federal Building
100 West Capitol Street
Jackson, MS 39269-1601
USSS 601.965.4436/601.965.4012
Federal Building
100 West Capitol Street, Suite 840
Jackson, MS 39269

MISSOURI
Kansas City
FBI 816.512.8200/816.512.8545
1300 Summit
Kansas City, MO 64105-1362
USSS 816.460.0600/816.283.0321
1150 Grand Avenue, Suite 510
Kansas City, MO 64106
Springfield
USSS 417.864.8340/417.864.8676
901 St. Louis Street, Suite 306
Springfield, MO 65806
St. Louis
FBI 314.231.4324/314.589.2636
222 Market Street
St. Louis, MO 63103-2516
USSS 314.539.2238/314.539.2567
Thomas F. Eagleton U.S. Courthouse
111 S. 10th Street, Suite 11.346
St. Louis, MO 63102

MONTANA
Great Falls
USSS 406.452.8515/406.761.2316
11 Third Street North
Great Falls, MT 59401

NEBRASKA
Omaha
FBI 402.493.8688/402.492.3799
10755 Burt Street
Omaha, NE 68114-2000
USSS 402.965.9670/402.445.9638
2707 North 108 Street, Suite 301
Omaha, NE 68164

NEVADA
Las Vegas
FBI 702.385.1281/702.385.1281
John Lawrence Bailey Building
700 East Charleston Boulevard
Las Vegas, NV 89104-1545
USSS 702.388.6571/702.388.6668
600 Las Vegas Boulevard South,
Suite 600
Las Vegas, NV 89101
Reno
USSS 775.784.5354/775.784.5991
100 West Liberty Street, Suite 850
Reno, NV 89501

NEW HAMPSHIRE
Manchester
USSS 603.626.5631/603.626.5653
1750 Elm Street, Suite 802
Manchester, NH 03104

NEW JERSEY
Atlantic City
USSS 609.487.1300/609.487.1491
Ventnor Professional Campus
6601 Ventnor Avenue
Ventnor City, NJ 08406
Newark
FBI 973.792.3000/973.792.3035
1 Gateway Center, 22nd Floor
Newark, NJ 07102-9889
USSS 973.656.4500/973.984.5822
Headquarters Plaza, West Towers,
Speedwell Avenue, Suite 700
Morristown, NJ 07960
Trenton
USSS 609.989.2008/609.989.2174
402 East State Street, Suite 3000
Trenton, NJ 08608

NEW MEXICO
Albuquerque
FBI 505.224.2000/505.224.2276
415 Silver Avenue SW, Suite 300
Albuquerque, NM 87102
USSS 505.248.5290/505.248.5296
505 Marquette Street NW
Albuquerque, NM 87102

FBI & USSS FIELD OFFICES

TELEPHONE/FAX
ADDRESS

NEW YORK

Albany
FBI 518.465.7551/518.431.7463
200 McCarty Avenue
Albany, NY 12209
USSS 518.436.9600/518.436.9635
39 North Pearl Street, 2nd Floor
Albany, NY 12207

Buffalo
FBI 716.856.780/716.843.5288
One FBI Plaza
Buffalo, NY 14202-2698
USSS 716.551.4401/716.551.5075
610 Main Street, Suite 300
Buffalo, NY 14202

JFK
USSS 718.553.0911/718.553.7626
John F. Kennedy Int'l. Airport
Building 75, Room 246
Jamaica, NY 11430

Melville
USSS 631.249.0404/631.249.0991
35 Pinelawn Road
Melville, NY 11747

New York
FBI 212.384.1000/212.384.2745
or 2746
26 Federal Plaza, 23rd Floor
New York, NY 10278-0004
USSS 212.637.4500/212.637.4687
335 Adams Street, 32nd Floor
Brooklyn, NY 11201

Rochester
USSS 716.263.6830/716.454.2753
Federal Building
100 State Street, Room 606
Rochester, NY 14614

Syracuse
USSS 315.448.0304/315.448.0302
James Hanley Federal Building
100 S. Clinton Street, Room 1371
Syracuse, NY 13261

White Plains
USSS 914.682.6300/914.682.6182
140 Grand Street, Suite 300
White Plains, NY 10601

NORTH CAROLINA

Charlotte
FBI 704.377.9200/704.331.4595
Wachovia Building
400 South Tyron Street, Suite 900
Charlotte, NC 28285-0001
USSS 704.442.8370/704.442.8369
One Fairview Center
6302 Fairview Road
Charlotte, NC 28210

Greensboro
USSS 336.547.4180/336.547.4185
4905 Koger Boulevard, Suite 220
Greensboro, NC 27407

Raleigh
USSS 919.790.2834/919.790.2832
4407 Bland Road, Suite 210
Raleigh, NC 27609

Wilmington
USSS 910.815.4511/910.815.4521
One Rodney Square
920 King Street, Suite 414
Wilmington, DE 19801

NORTH DAKOTA

Fargo
USSS 701.239.5070/701.239.5071
657 2nd Avenue North, Suite 302A
Fargo, ND 58102

OHIO

Cincinnati
FBI 513.421.4310/513.562.5650
John Weld Peck Federal Building
550 Main Street, Room 9000
Cincinnati, OH 45202-8501
USSS 513.684.3585/513.684.3436
John Weld Peck Federal Building
550 Main Street
Cincinnati, OH 45202

Cleveland
FBI 216.522.1400/216.622.6717
Federal Office Building
1240 East 9th Street, Room 3005
Cleveland, OH 44199-9912
USSS 216.706.4365/216.706.4445
6100 Rockside Woods Boulevard
Suite 440
Cleveland, OH 44131-2334

Columbus
USSS 614.469.7370/614.469.2049
500 South Front Street, Suite 800
Columbus, OH 43215

Dayton
USSS 937.225.2900/937.225.2724
Federal Building
200 West Second Street, Room 811
Dayton, OH 45402

Toledo
USSS 419.259.6434/419.259.6437
4 Seagate Center, Suite 702
Toledo, OH 43604

OKLAHOMA

Oklahoma City
FBI 405.290.7770/405.290.3885
3301 West Memorial Drive
Oklahoma City, OK 73134
USSS 405.810.3000/405.810.3098
Lakepoint Towers
4013 NW Expressway, Suite 650
Oklahoma City, OK 73116

Tulsa
USSS 918.581.7272
Pratt Tower
125 West 15th Street, Suite 400
Tulsa, OK 74119

OREGON

Portland
FBI 503.224.4181/503.552.5400
Crown Plaza Building
1500 SW 1st Avenue, Suite 400
Portland, OR 97201-5828
USSS 503.326.2162/503.326.3258
1001 SW 5th Avenue, Suite 1020
Portland, OR 97204

PENNSLYVANIA

Philadelphia
FBI 215.418.4000/215.418.4232
William J. Green Jr. Federal
Office Building
600 Arch Street, 8th Floor
Philadelphia, PA 19106
USSS 215.861.3300/215.861.3311
7236 Federal Building
600 Arch Street
Philadelphia, PA 19106

Pittsburgh
FBI 412.471.2000/412.432.4188
U.S. Post Office Building
700 Grant Street, Suite 300
Pittsburgh, PA 15219-1906
USSS 412.395.6484/412.395.6349
1000 Liberty Avenue
Pittsburgh, PA 15222

Scranton
USSS 570.346.5781/570.346.3003
235 N. Washington Avenue, Suite 247
Scranton, PA 18501

RHODE ISLAND

Providence
USSS 401.331.6456/401.528.4394
The Federal Center
380 Westminster Street, Suite 343
Providence, RI 02903

SOUTH CAROLINA

Charleston
USSS 843.747.7242/843.747.7787
5900 Core Avenue, Suite 500
North Charleston, SC 29406

Columbia
FBI 803.551.4200/803.551.4324
151 Westpark Boulevard
Columbia, SC 29210-3857
USSS 803.765.5446/803.765.5445
1835 Assembly Street, Suite 1425
Columbia, SC 29201

Greenville
USSS 864.233.1490/864.235.6237
NCNB Plaza
7 Laurens Street, Suite 508
Greenville, SC 29601

SOUTH DAKOTA

Sioux Falls
USSS 605.330.4565/605.330.4523
230 South Phillips Avenue, Suite 405
Sioux Falls, SD 57104

TENNESSEE

Chattanooga
USSS 423.752.5125/423.752.5130
Post Office Building
900 Georgia Avenue, Room 204
Chattanooga, TN 37402

Knoxville
FBI 865.544.0751/865.544.3590
John J. Duncan Federal Office Building
710 Locust Street, Suite 600
Knoxville, TN 37902-2537
USSS 865.545.4627/865.545.4633
John J. Duncan Federal Office Building
710 Locust Street, Room 517
Knoxville, TN 37902

Memphis
FBI 901.747.4300/901.747.9621
Eagle Crest Building
225 North Humphreys Boulevard,
Suite 3000
Memphis, TN 38120-2107
USSS 901.544.0333/901.544.0342
5350 Poplar Avenue, Suite 204
Memphis, TN 38119

Nashville
USSS 615.736.5841/615.736.5848
658 U.S. Courthouse
801 Broadway Street
Nashville, TN 37203

FBI & USSS FIELD OFFICES

TELEPHONE/FAX
ADDRESS

TEXAS

Austin
USSS 512.916.5103/512.916.5365
Federal Office Building
300 E. 8th Street
Austin, TX 78701

Dallas
FBI 214.720.2200/214.922.7459
1801 North Lamar, Suite 300
Dallas, TX 75202-1795
USSS 972.868.3200/972.868.3232
125 East John W. Carpenter Freeway,
Suite 300
Irving, TX 75062

El Paso
FBI 915.832.5000/915.832.5259
660 S. Mesa Hills Drive
El Paso, TX 79912
USSS 915.533.6950/915.533.8646
Mesa One Building
4849 North Mesa, Suite 210
El Paso, TX 79912

Houston
FBI 713.693.5000/713.693.3999
2500 East TC Jester
Houston, TX 77008-1300
USSS 713.868.2299/713.868.5093
602 Sawyer Street, Suite 500
Houston, TX 77007

Lubbock
USSS 806.472.7347/806.472.7542
1205 Texas Avenue, Room 813
Lubbock, TX 79401

McAllen
USSS 956.630.5811/956.630.5838
200 S. 10th Street, Suite 1107
McAllen, TX 78501

San Antonio
FBI 210.225.6741/210.978.5380
U.S. Post Office Building
615 East Houston Street, Suite 200
San Antonio, TX 78205-9998
USSS 210.472.6175/210.472.6185
727 East Durango Boulevard,
Suite B410
San Antonio, TX 78206-1265

Tyler
USSS 903.534.2933 903.581.9569
6101 South Broadway, Suite 395
Tyler, TX 75703

UTAH

Salt Lake City
FBI 801.579.1400/801.579.4500
257 Towers Building
257 East 200 South, Suite 1200
Salt Lake City, UT 84111-2048
USSS 801.524.5910/801.524.6216
57 West 200 South Street, Suite 450
Salt Lake City, UT 84101

VERMONT
FBI 518.465.7551/518.431.7463
Contact field office located in
Albany, NY
USSS 617.565.5640/617.565.5659
Contact field office located in
Boston, MA

VIRGINIA

Norfolk
FBI 757.455.0100/757.455.2647
150 Corporate Boulevard
Norfolk, VA 23502-4999
USSS 757.441.3200/757.441.3811
Federal Building
200 Granby Street, Suite 640
Norfolk, VA 23510

Richmond
FBI 804.261.1044/804.627.4494
1970 East Parham Road
Richmond, VA 23228
USSS 804.771.2274/804.771.2076
600 East Main Street, Suite 1910
Richmond, VA 23219

Roanoke
USSS 540.345.4301/540.857.2151
105 Franklin Road SW, Suite 2
Roanoke, VA 24011

WASHINGTON

Seattle
FBI 206.622.0460/206.262.2587
1110 Third Avenue
Seattle, WA 98101
USSS 206.220.6800/206.220.6479
890 Federal Building
915 Second Avenue
Seattle, WA 98174

Spokane
USSS 509.353.2532/509.353.2871
601 W. Riverside Avenue, Suite 1340
Spokane, WA 99201

WEST VIRGINIA

Charleston
USSS 304.347.5188/304.347.5187
5900 Core Avenue, Suite 500
North Charleston, SC 29406

WISCONSIN

Madison
USSS 608.264.5191/608.264.5592
131 W. Wilson Street, Suite 303
Madison, WI 53703

Milwaukee
FBI 414.276.4684/414.276.6560
330 East Kilbourn Avenue
Milwaukee, WI 53202
USSS 414.297.3587/414.297.3595
572 Courthouse
517 E. Wisconsin Avenue
Milwaukee, WI 53202

WYOMING

Cheyenne
USSS 307.772.2380/307.772.2387
2120 Capitol Avenue, Suite 3026
Cheyenne, WY 82001

The U.S. Secret Service notes that the Electronic Crimes Branch of the USSS Headquarters in Washington, D.C., is ready to field questions and/or accept computer intrusion reports. Tel: (202) 406-5850. Fax: (202) 406-5031. Online: www.treas.gov/usss.

The FBI notes computer intrusion reports may also be submitted to the National Infrastructure Protection Center. Tel: (202) 323-3205; (888) 585-9078. Fax: (202) 323-2079. Email: nipc.watch@fbi.gov. Online: www.nipc.gov/incident/cirr.htm.

Additional investigative programs may exist within your local law enforcement community (i.e., city, county or state police, district attorney investigative units, and/or state attorney generals' offices).

CIO CYBERTHREAT REPORT FORM

This form outlines the basic information law enforcement needs on a first call. You can use it as an internal worksheet or fill it out and e-mail or fax it to law enforcement. Additional data that will help agents in their investigation is outlined in the CIO Cyberthreat Response & Reporting Guidelines, but the best way to determine what will be most helpful to investigators in the event of an attack is to ask.

STATUS

☐ Site Under Attack ☐ Past Incident ☐ Repeated Incidents, unresolved

CONTACT INFORMATION

Name_____Title_____

Organization_____

Direct-Dial Phone_____E-mail_____

Legal Contact Name_____Phone_____

Location/Site(s) Involved_____

Street Address_____

City_____State_____IP_____

Main Telephone_____Fax_____

ISP Contact Information_____

INCIDENT DESCRIPTION

☐ Denial of Service
☐ Distributed Denial of Service
☐ Malicious Code (virus, worm)
☐ Intrusion/Hack
☐ Other (specify)_____
☐ Unauthorized Electronic Monitoring (sniffers)
☐ Misuse of Systems (internal or external)
☐ Website Defacement
☐ Probe/Scan

DATE/TIME OF INCIDENT DISCOVERY

Date_____Time_____

Duration of Attack_____

IMPACT OF ATTACK

☐ Loss/Compromise of Data
☐ System Downtime
☐ Damage to Systems
☐ Financial Loss (estimated amount: >$_____)
☐ Damage to the Integrity or Delivery of Critical Goods, Services or Information
☐ Other Organizations' Systems Affected

SEVERITY OF ATTACK, INCLUDING FINANCIAL LOSS, INFRASTRUCTURE, PR IMPACT IF MADE PUBLIC

☐ High ☐ Medium ☐ Low ☐ Unknown

SENSITIVITY OF DATA

☐ High ☐ Medium ☐ Low ☐ Unknown

How did you detect this?_____

Have you contacted law enforcement about this incident before? Who & when?_____

Has the incident been resolved? Explain_____

CONTRIBUTORS

INDUSTRY

Peter Allor
Manager, ISAC Operations
Special Operations Group, X-Force
Internet Security Systems, Inc.

Bruce Moulton
Past Chairman & Current Advisor
Financial Services ISAC

John Puckett
VP and General Manager, Wireless and Internet Technologies
Polaroid Corp.

Howard Schmidt
Vice Chair
President's Critical Infrastructure Board
and former Chief Security Officer
Microsoft Corp.

Alan Sonnenberg
Senior Director/Engineering and Security, Wireless and Internet Technologies
Polaroid Corp.

Michael Young
Principal & Chief Information Security Officer
State Street Global Advisors

UNITED STATES LAW ENFORCEMENT

Steven Chabinsky
Principal Legal Advisor, National Infrastructure Protection Center & Assistant General Counsel, Office of the General Counsel, *FBI*

Steve Colo
Assistant Director
U.S. Secret Service

Ronald L. Dick
Director, National Infrastructure Protection Center &
Deputy Assistant Director, Counterterrorism Division, *FBI*

Paul Irving
Assistant Director for Government and Public Affairs
U.S. Secret Service

James Savage
Deputy Special Agent in Charge
U.S. Secret Service
Financial Crimes Division

Bruce A. Townsend
Special Agent in Charge
U.S. Secret Service
Financial Crimes Division

CXO MEDIA

Abbie Lundberg
Editor in Chief,
CIO *Magazine*

Lori Piscatelli
News & Information Assistant

Susan Watson
VP, News & Information

ADDITIONAL REVIEWERS

Steven Agnoli
CIO
Kirkpatrick & Lockhart LLP

William Crowell
Former CIO
Meredith Corp.

Patrick Gray
Manager, Internet Threat Intelligence Center
Special Operations Group, X-Force
Internet Security Systems, Inc.

Scott Hicar
CIO
Maxtor Corp.

Paul Ingevaldson
SVP, Technology and International Operations
Ace Hardware

Scott Kelly
VP of IT
Symtx

Frank O'Connor
CIO
ECom Systems, Inc.

Steven Steinbrecher
CIO
Contra Costa County

Glenn West
Vice President, IT Services
Long John Silvers

Marc West
CIO
Electronic Arts

Ed Winfield
CIO
FX Coughlin Co.