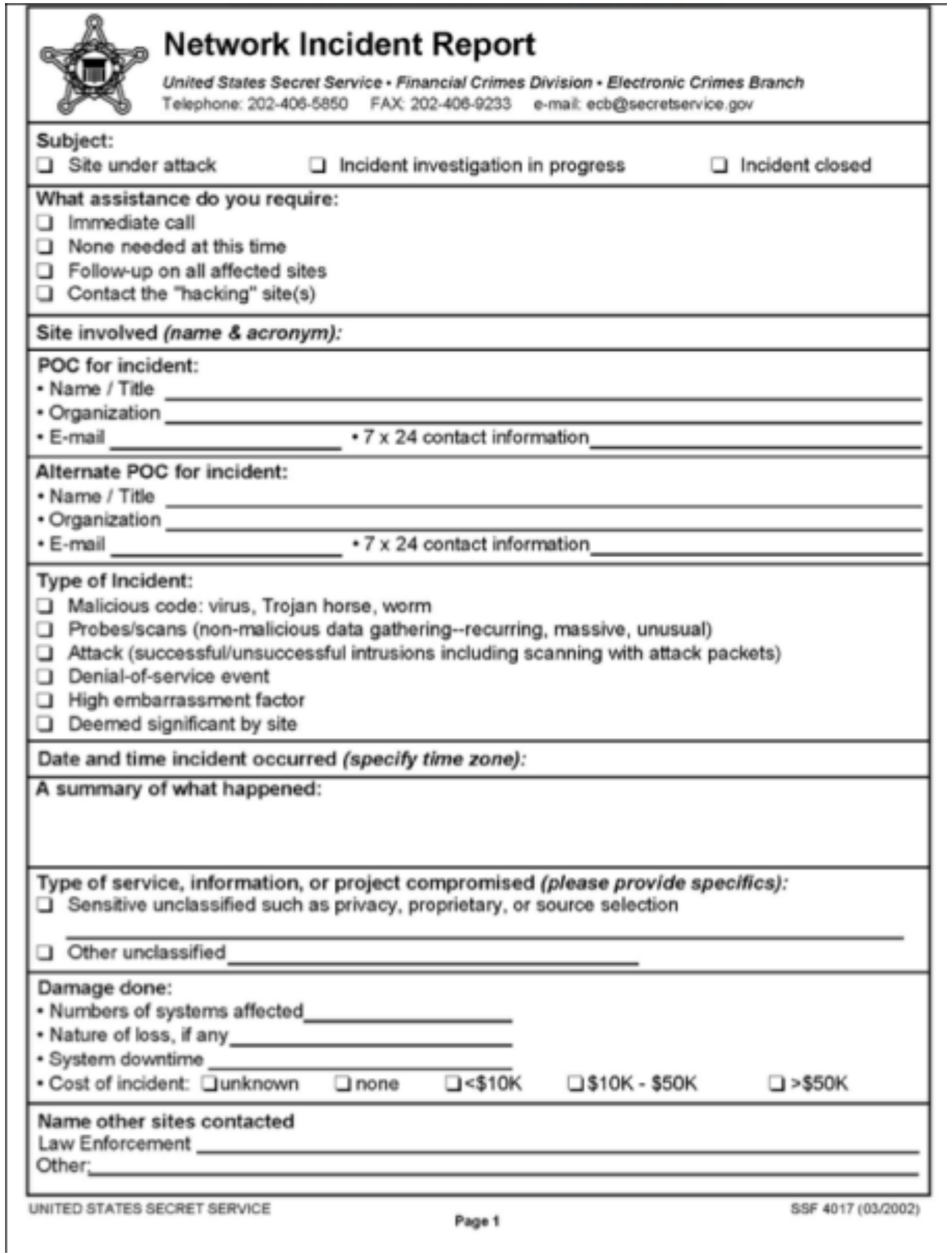
- No Starch Press: www.nostarch.com
- DHS National Checklist Program Repository: http://web.nvd.nist.gov/view/ncp/repository
- NIST Special Publications: http://csrc.nist.gov/publications/nistpubs/index.html
- Microsoft Security Guides for Security Compliance Management Toolkit Series: http://technet.microsoft.com/en-us/library/cc677002.aspx

Appendix B: Incident Response Report



Network Incident Report

United States Secret Service • Financial Crimes Division • Electronic Crimes Branch
Telephone: 202-406-5850 FAX: 202-406-9233 e-mail: ecb@secretservice.gov

Subject:
❑ Site under attack ❑ Incident investigation in progress ❑ Incident closed

What assistance do you require:
❑ Immediate call
❑ None needed at this time
❑ Follow-up on all affected sites
❑ Contact the "hacking" site(s)

Site involved *(name & acronym):*

POC for incident:
• Name / Title ____________________
• Organization ____________________
• E-mail ____________ • 7 x 24 contact information ____________

Alternate POC for incident:
• Name / Title ____________________
• Organization ____________________
• E-mail ____________ • 7 x 24 contact information ____________

Type of Incident:
❑ Malicious code: virus, Trojan horse, worm
❑ Probes/scans (non-malicious data gathering--recurring, massive, unusual)
❑ Attack (successful/unsuccessful intrusions including scanning with attack packets)
❑ Denial-of-service event
❑ High embarrassment factor
❑ Deemed significant by site

Date and time incident occurred *(specify time zone):*

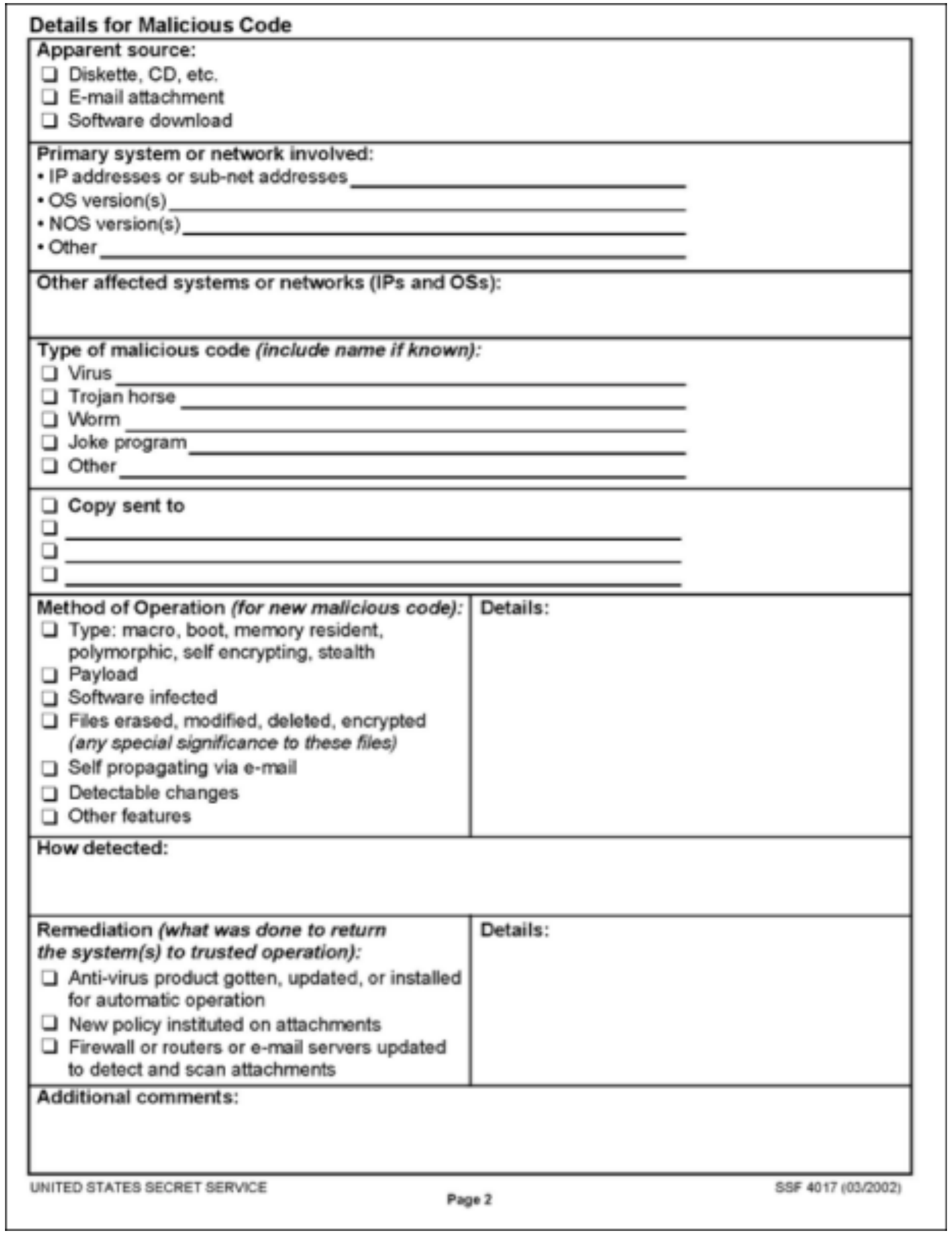
A summary of what happened:

Type of service, information, or project compromised *(please provide specifics):*
❑ Sensitive unclassified such as privacy, proprietary, or source selection
____
❑ Other unclassified ____________________

Damage done:
• Numbers of systems affected ____________
• Nature of loss, if any ____________
• System downtime ____________
• Cost of incident: ❑unknown ❑none ❑<$10K ❑$10K - $50K ❑>$50K

Name other sites contacted
Law Enforcement ____________________
Other: ____________________

UNITED STATES SECRET SERVICE Page 1 SSF 4017 (03/2002)



Details for Malicious Code

Apparent source:
- ❑ Diskette, CD, etc.
- ❑ E-mail attachment
- ❑ Software download

Primary system or network involved:
- • IP addresses or sub-net addresses ____________
- • OS version(s) ____________
- • NOS version(s) ____________
- • Other ____________

Other affected systems or networks (IPs and OSs):

Type of malicious code *(include name if known)*:
- ❑ Virus ____________
- ❑ Trojan horse ____________
- ❑ Worm ____________
- ❑ Joke program ____________
- ❑ Other ____________

❑ **Copy sent to**
- ❑ ____________
- ❑ ____________
- ❑ ____________

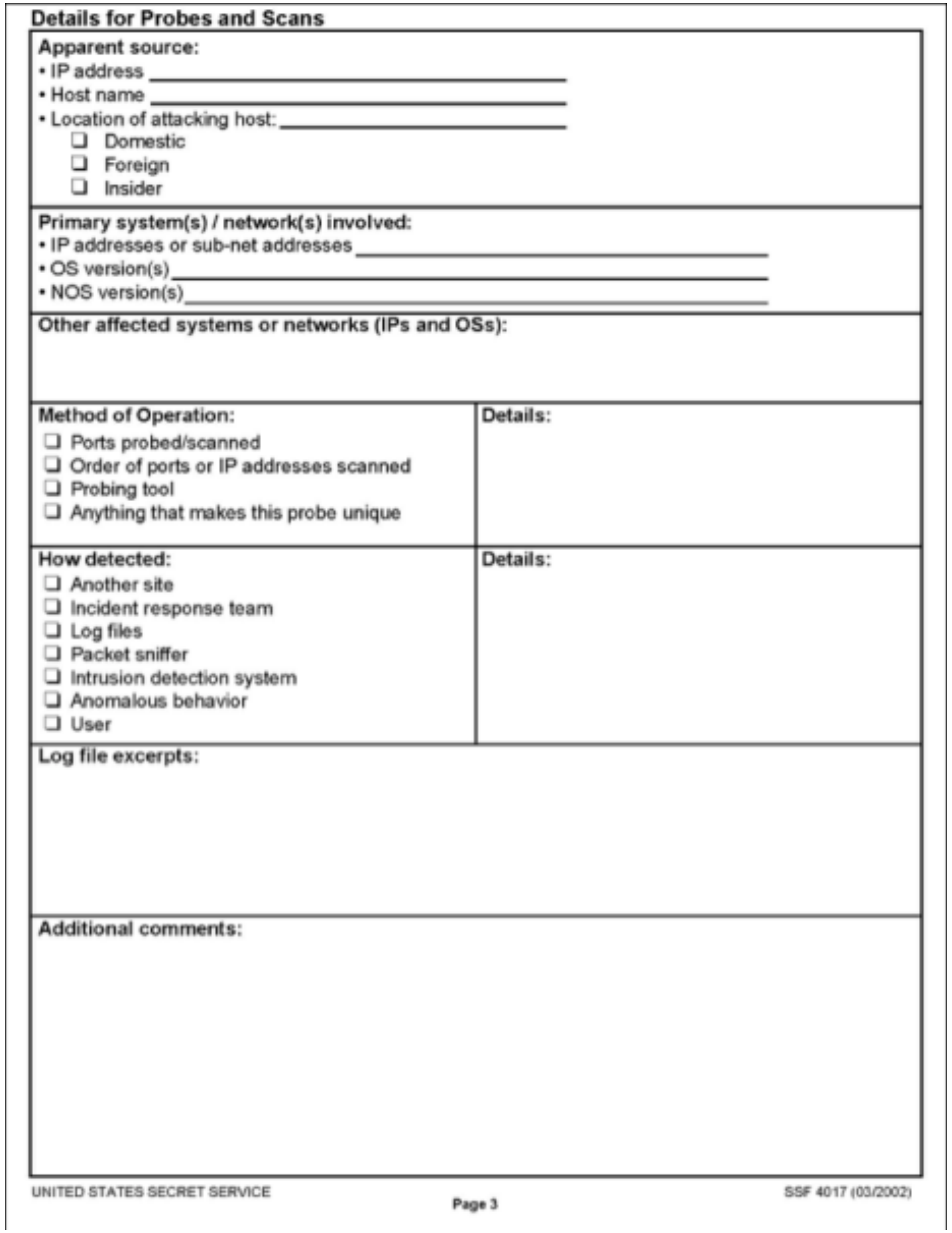
Method of Operation *(for new malicious code)*: ❑ Type: macro, boot, memory resident, polymorphic, self encrypting, stealth ❑ Payload ❑ Software infected ❑ Files erased, modified, deleted, encrypted *(any special significance to these files)* ❑ Self propagating via e-mail ❑ Detectable changes ❑ Other features	**Details:**

How detected:

Remediation *(what was done to return the system(s) to trusted operation)*: ❑ Anti-virus product gotten, updated, or installed for automatic operation ❑ New policy instituted on attachments ❑ Firewall or routers or e-mail servers updated to detect and scan attachments	**Details:**

Additional comments:

UNITED STATES SECRET SERVICE Page 2 SSF 4017 (03/2002)



Details for Probes and Scans

Apparent source:
- • IP address ____________
- • Host name ____________
- • Location of attacking host: ____________
  - ❑ Domestic
  - ❑ Foreign
  - ❑ Insider

Primary system(s) / network(s) involved:
- • IP addresses or sub-net addresses ____________
- • OS version(s) ____________
- • NOS version(s) ____________

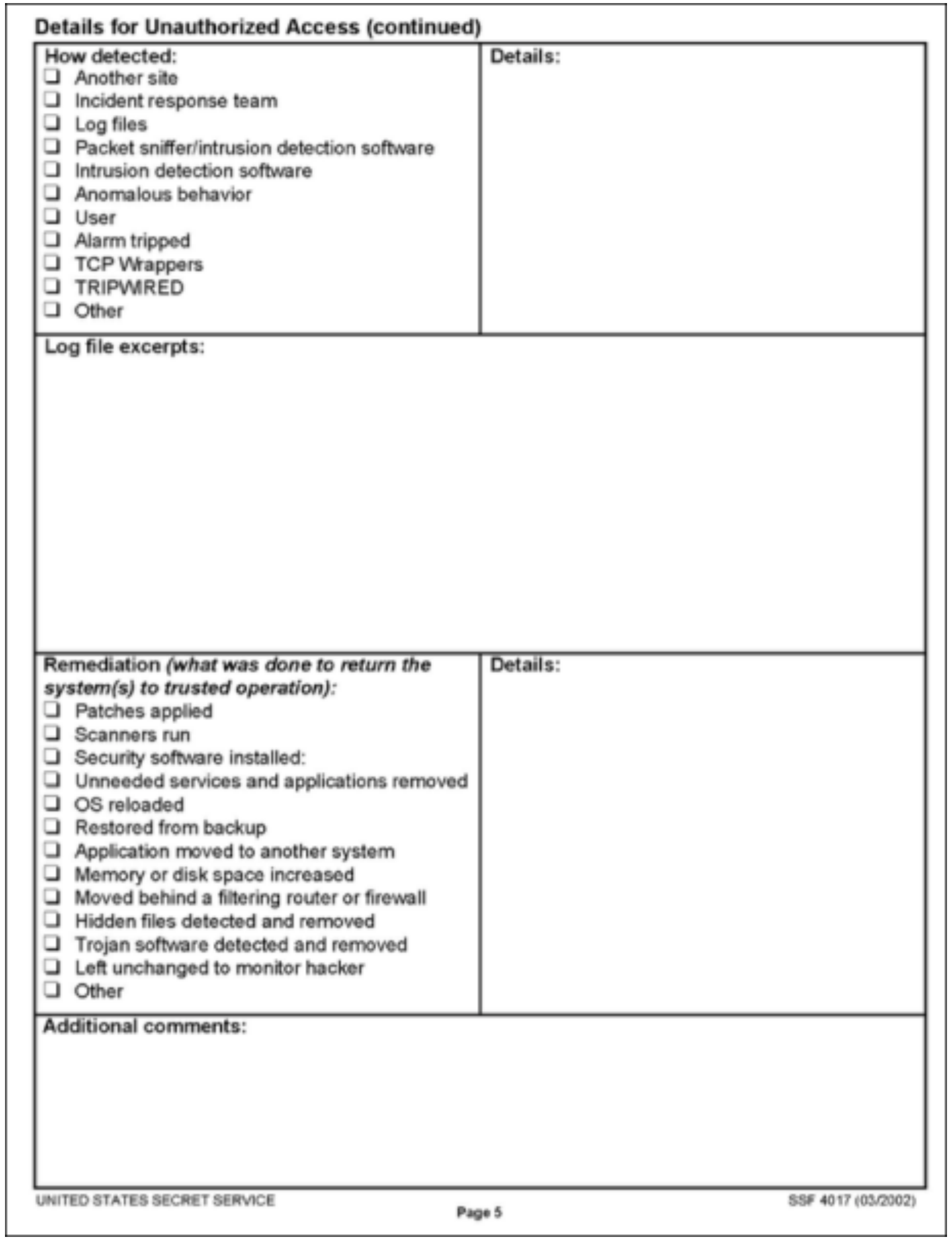
Other affected systems or networks (IPs and OSs):

Method of Operation: ❑ Ports probed/scanned ❑ Order of ports or IP addresses scanned ❑ Probing tool ❑ Anything that makes this probe unique	**Details:**
How detected: ❑ Another site ❑ Incident response team ❑ Log files ❑ Packet sniffer ❑ Intrusion detection system ❑ Anomalous behavior ❑ User	**Details:**

Log file excerpts:

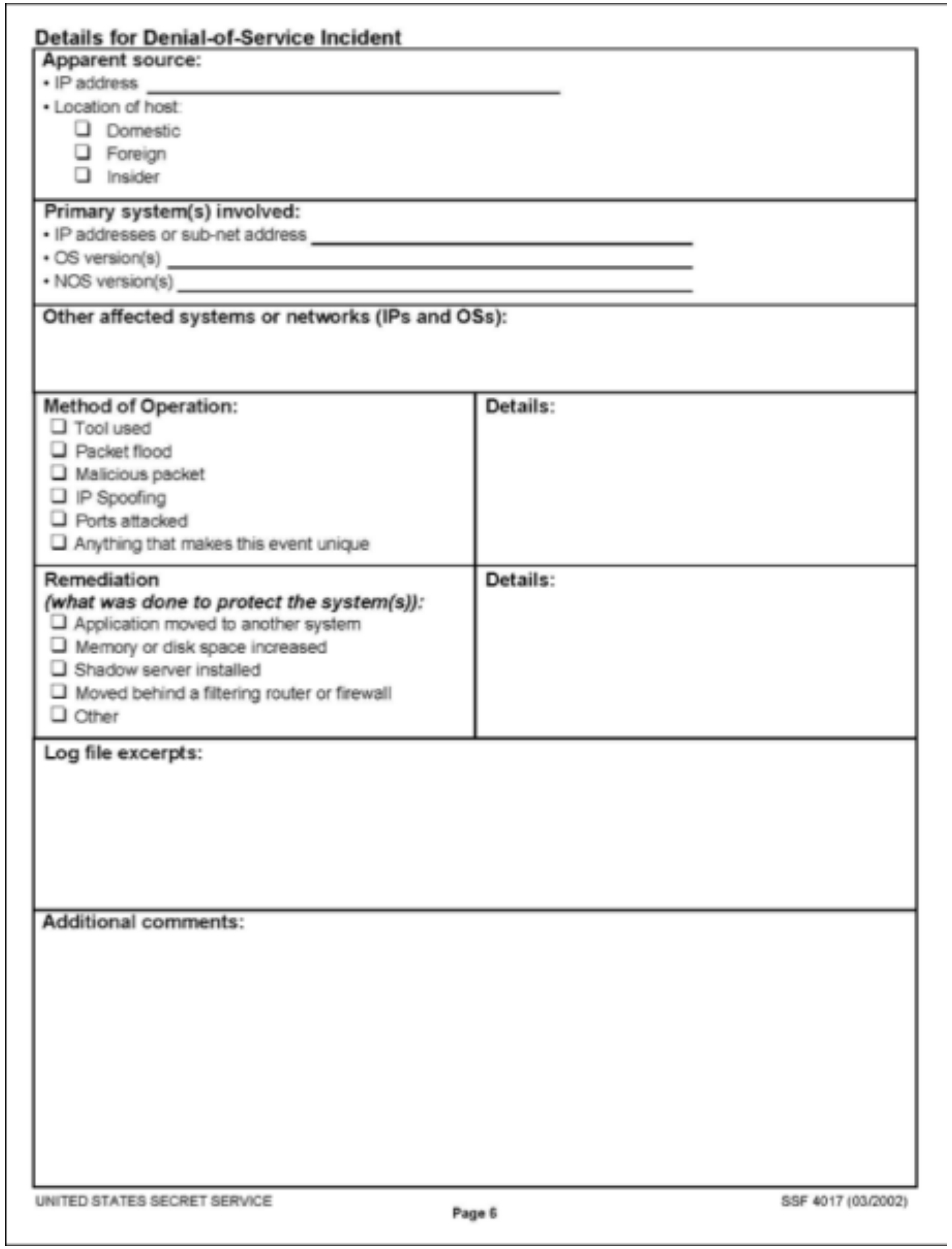
Additional comments:

UNITED STATES SECRET SERVICE Page 3 SSF 4017 (03/2002)



Details for Unauthorized Access (continued)

How detected: ❑ Another site ❑ Incident response team ❑ Log files ❑ Packet sniffer/intrusion detection software ❑ Intrusion detection software ❑ Anomalous behavior ❑ User ❑ Alarm tripped ❑ TCP Wrappers ❑ TRIPWIRED ❑ Other	**Details:**
Log file excerpts:	
Remediation ***(what was done to return the system(s) to trusted operation):*** ❑ Patches applied ❑ Scanners run ❑ Security software installed: ❑ Unneeded services and applications removed ❑ OS reloaded ❑ Restored from backup ❑ Application moved to another system ❑ Memory or disk space increased ❑ Moved behind a filtering router or firewall ❑ Hidden files detected and removed ❑ Trojan software detected and removed ❑ Left unchanged to monitor hacker ❑ Other	**Details:**
Additional comments:	



Details for Denial-of-Service Incident

Apparent source: • IP address ____________________ • Location of host: ❑ Domestic ❑ Foreign ❑ Insider	
Primary system(s) involved: • IP addresses or sub-net address ____________________ • OS version(s) ____________________ • NOS version(s) ____________________	
Other affected systems or networks (IPs and OSs):	
Method of Operation: ❑ Tool used ❑ Packet flood ❑ Malicious packet ❑ IP Spoofing ❑ Ports attacked ❑ Anything that makes this event unique	**Details:**
Remediation ***(what was done to protect the system(s)):*** ❑ Application moved to another system ❑ Memory or disk space increased ❑ Shadow server installed ❑ Moved behind a filtering router or firewall ❑ Other	**Details:**
Log file excerpts:	
Additional comments:	