DOCID: 3967120
The opinions expressed in this article are those of the author(s) and do not represent the official opinion of NSA/CSS.

~~SECRET~~

Out of Control (U)

[redacted] P.L. 86-36

INTRODUCTION (U)

(U) In their quest to benefit from the great advantages of networked computer systems, the U.S. military and intelligence communities have put almost all of their classified information "eggs" into one very precarious basket: computer system administrators. A relatively small number of system administrators are able to read, copy, move, alter, and destroy almost every piece of classified information handled by a given agency or organization. An insider-gone-bad with enough hacking skills to gain root privileges might acquire similar capabilities. It seems amazing that so few are allowed to control so much – apparently with little or no supervision or security audits. The system administrators might audit users, but who audits *them*? Even if higher level auditing of system administrators takes place, it is unlikely that such audits are frequent enough or extensive enough to be effective, especially against experts who probably know their systems better than their auditors.

~~(S-UO)~~ This is not meant as an attack on the integrity of system administrators as a whole, nor is it an attempt to blame anyone for this gaping vulnerability. It is, rather, a warning that system administrators are likely to be targeted – increasingly targeted – by foreign intelligence services because of their special access to information. This is especially true for the system administrators of classified networks. Historical evidence of foreign intelligence targeting of U.S. communicators – people who had special access to cryptographic material – strongly supports this assertion.

(U) This situation also raises a concern about individual accountability for classified information. In short, individual users have lost control over access to electronic versions of their classified files. If the next Aldrich Ames turns out to be a system administrator who steals and sells classified reports stored on-line by analysts or other users, will the users be liable in any way? Clearly, steps must be taken to counter the threat to system administrators and to ensure individual accountability for classified information that is created, processed, or stored electronically.

COMMUNICATORS HAVE BEEN HEAVILY TARGETED FOR THEIR ACCESS TO KEY ~~(S-UO)~~

~~(S-UO)~~ During the Cold War, untold numbers of people were recruited by Soviet Bloc intelligence services to spy against the U.S. and the West, but among the most prized agents were U.S. communicators or others who could supply cryptographic material and related information. Between 1946 and 1986, [redacted] U.S. government

Declassified and approved for release by NSA on 03-23-2011 pursuant to E.O. 13526

DOCID: 3967120

personnel were known to compromise U.S. cryptographic systems on behalf of foreign intelligence services, primarily those of the Soviet Union. Many other individuals also provided U.S. key to foreign intelligence services but were never formally charged. Crypto key was (and still is) hot stuff because acquiring it – especially through an agent – was the easiest way that the bad guys could gain access to hundreds or even thousands of classified U.S. messages.

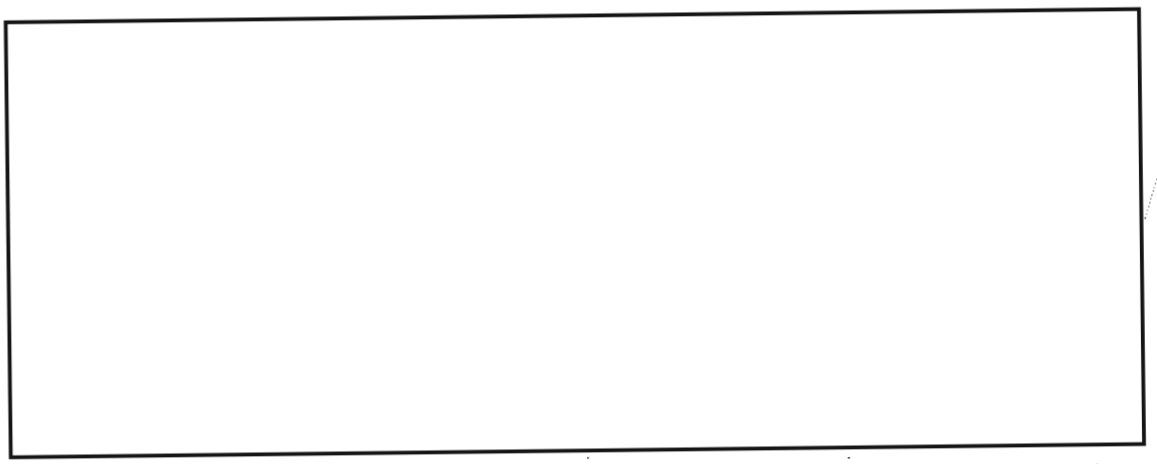
SYSTEM ADMINISTRATORS ARE POTENTIALLY MORE LUCRATIVE HUMINT TARGETS THAN COMMUNICATORS ~~(S-UO)~~

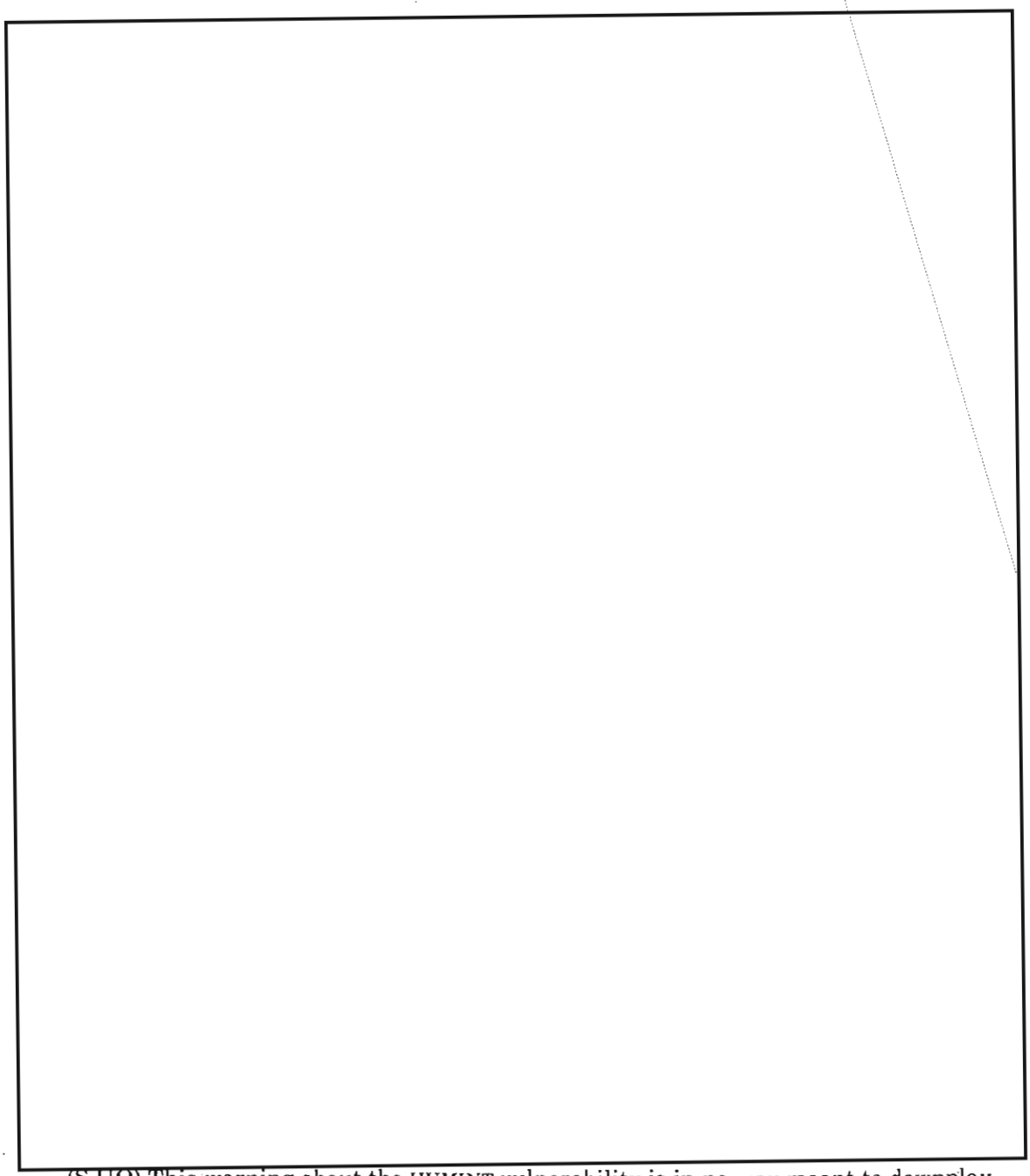
~~(S-UO)~~ With system administrators, though, the situation is potentially much worse than it has ever been with communicators. In part, this is because the system administrators can so easily, so quickly, so *undetectably*, steal vast quantities of information. Communicators of the past usually sent only relatively short messages and "finished" documents, but today's system administrators can obtain full-length copies of entire reports, including draft versions, as well as informal e-mail messages, electronic calendar appointments, and a wide variety of other data.

(U) In some cases, they might even be able to mount what are called close-in technical attacks by remotely activating workstation microphones, effectively turning them into audio "bugs." They also have the ability to acquire and pre-sort high-quality information, which saves the foreign intelligence service time and resources that would otherwise be devoted to sorting through bulk collection. Furthermore, system administrators are capable of manipulation – destroying or altering data and controlling the availability of networks or specific applications.

FOREIGN INTELLIGENCE SERVICES ARE ALREADY TARGETING COMPUTER PERSONNEL ~~(S-UO)~~

EO 1.4.(c)
P.L. 86-36





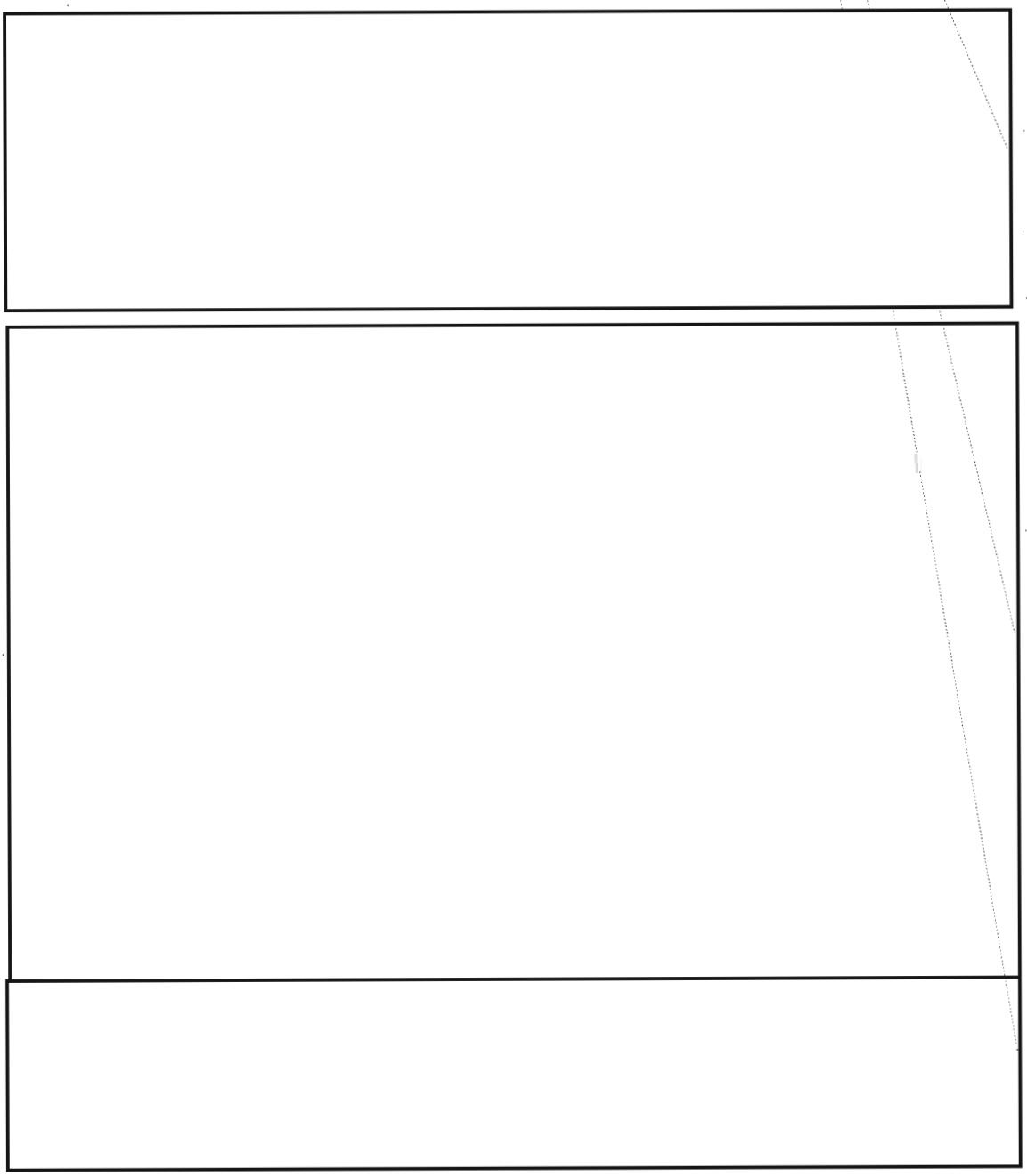
~~(S//NF)~~ This warning about the HUMINT vulnerability is in no way meant to downplay the need for stringent technical security solutions, but just as unbreakable U.S. cryptography has pushed foreign intelligence services to target the people who control the key, so too will stronger network security spur increased targeting of the people who control the computers.

DOCID: 3967120

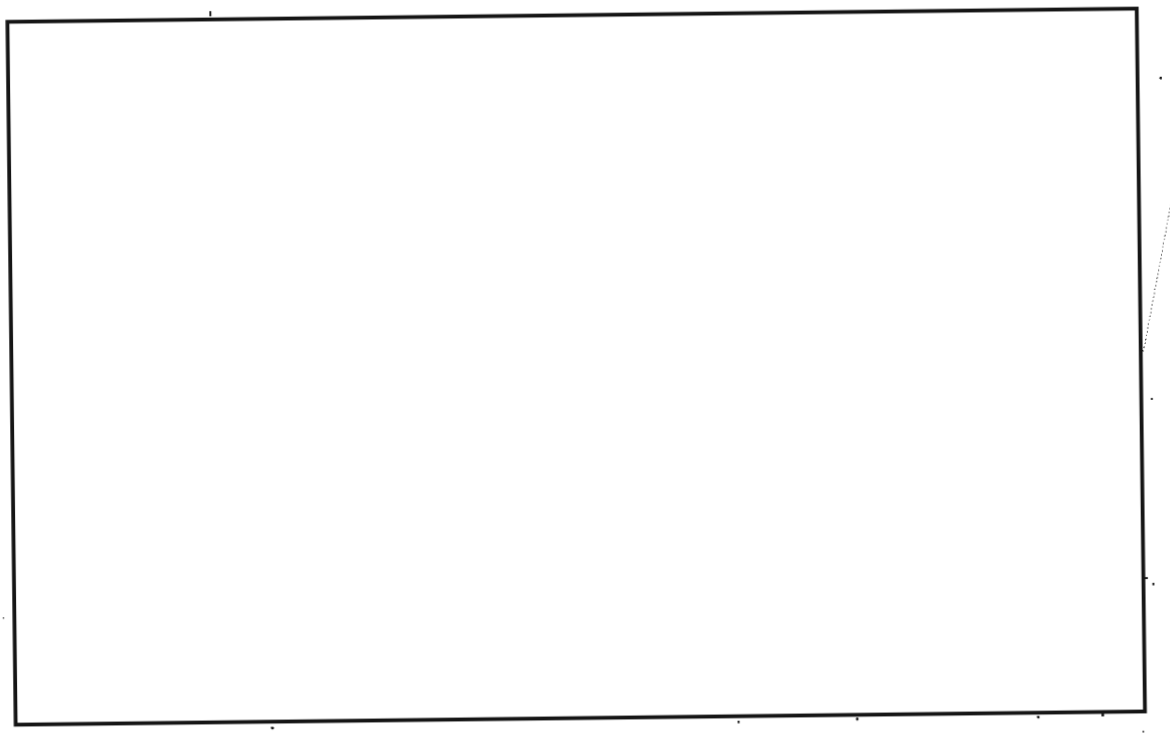
EO 1.4.(c)
EO 1.4.(g)
P.L. 86-36

THE NEED FOR MORE INDIVIDUAL ACCOUNTABILITY (U)

(U) This threat highlights the need to control classified electronic files, but, as most users of classified client-server networks already know, individuals have far less control over their own classified electronic files than they have over their hard copy documents. In short, people are doing things with electronic copies of classified information that would never be allowed with paper. For example, if a file is sent to the printer and does not print out, it is assumed to be a "glitch" – not a "lost" copy of a classified report.



DOCID: 3967120



EO 1.4.(c)
EO 1.4.(g)
P.L. 86-36

(U) These are troubling questions because, even though the vast majority of intelligence personnel are not system administrators, they are still legally, professionally, and morally responsible for the classified information that they produce, handle, or store. Users of classified systems must, therefore, be given greater control – individually – over the electronic versions of their notes, reports, and other documents. The information at risk includes

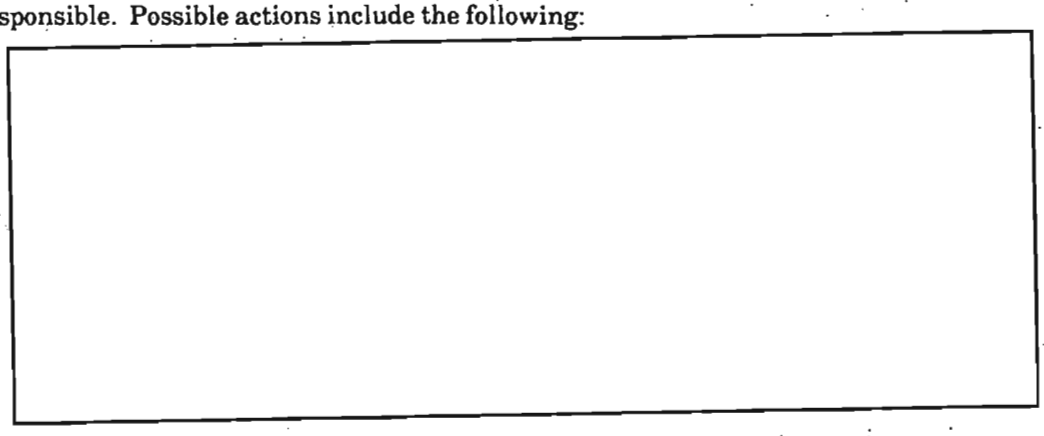
- widely disseminated classified and sensitive-but-unclassified documents;
- highly compartmented information with very strict need to know;
- information protected by the privacy act, such as personnel files, medical records, and security files;
- other highly sensitive information, such as Inspector General investigations and security investigations for counterintelligence or law enforcement matters.

CONCLUSIONS AND RECOMMENDATIONS (U)

~~(C)~~ The growing threat to system administrators heightens the need for accountability for classified electronic information, but there is no one easy answer to this problem. Most users enjoy and appreciate new technology and all of the associated benefits, from e-mail to bulletin boards to Web browsers to cost-saving shared resources. It is unlikely that anyone wants to return to the pre-client-server era, even if it were possible to do so. Still the military and intelligence communities must do *something* if they are to reestablish

DOCID: 3967120
E.O. 13526, 1.4.(c)
E.O. 13526, 1.4.(g)
P.L. 86-36

individual employees' control over the information for which they are personally responsible. Possible actions include the following:



(U) *Allow physical separations from networks.* Allow each workstation to function as both a stand-alone and a network terminal, with a physical disconnect from the LAN or other network. People who need to work on highly sensitive matters could thus do so with less anxiety about network attacks by physically disconnecting from their LAN. To be effective, this would require the more expensive installation of word processing or other applications on each workstation – rather than as a shared network resource using "licenses" – but it would also allow people to be productive during network down time. Of course, connecting to the network to send e-mail or surf the Web would have to be a relatively quick and easy procedure – such as plugging in a cable and then clicking on an icon.

~~(FOUO)~~ *Provide encryptable hard drives.* Analysts and managers should be able to store information on their own workstations' individual hard drives in an encrypted form that cannot be decrypted by anyone else, including system administrators. Yes, some people will forget a password or something and end up losing an important file, but that is the price of individual responsibility. Those analysts who do highly compartmented or otherwise sensitive work should be provided with removable hard drives that can be encrypted and stored in a three-combo safe. It would be preferable if, in the future, all hard drives could be removed for storage in a safe to prevent theft or damage from fire or other disasters. But then exit inspections would have to be reinstituted to help prevent people from carrying the drives out. An alternative would be to install sensors at each exit and tag each drive with a trigger mechanism, similar to the technology used by stores to combat shoplifting.

~~(FOUO)~~ *Give M5 and other security organizations more money.* It is unwise to cut security budgets now, and it's not only because of the threat of a specially equipped Ryder rental van taking out half of the FANX III building. Overall, employee susceptibility to foreign intelligence recruitment has probably increased in this era of unprecedented budget cuts and the accompanying low morale. In the long-term, security acts as a force-multiplier because it limits

DOCID: 3967120

otherwise exponential losses caused by spies, and good budget planners know that force multipliers should not be cut at the same rate as regular forces during downsizing.

[redacted] EO 1.4.(c) EO 1.4.(g) P.L. 86-36

[redacted]

~~(FOUO)~~ [redacted] **He is the primary editor of the *National INFOSEC Intelligence Review* (NIIR), published aperiodically by V52, and the *ISSO Global Threat Summary*, a reference manual also published by V52. He joined the Agency in 1986 and was professionalized as an Intelligence Research (IR) Analyst in 1990 after graduating from the IR intern program. He has an M.A. in national security studies from Georgetown University and a B.A. in foreign affairs from the University of Virginia. He holds memberships in the National Military Intelligence Association, the Association of Old Crows, and the International Affairs Institute. He was formerly a chapter president of Pi Sigma Alpha, the National Political Science Honor Society. He is an award-winning essayist and has published several articles in professional journals at NSA and CIA.**

P.L. 86-36

Derived from: NSA/CSSM 123-2, Dated 3 September 1991
Declassify On: Source Marked "OADR" Date of Source: 3 Sep 91