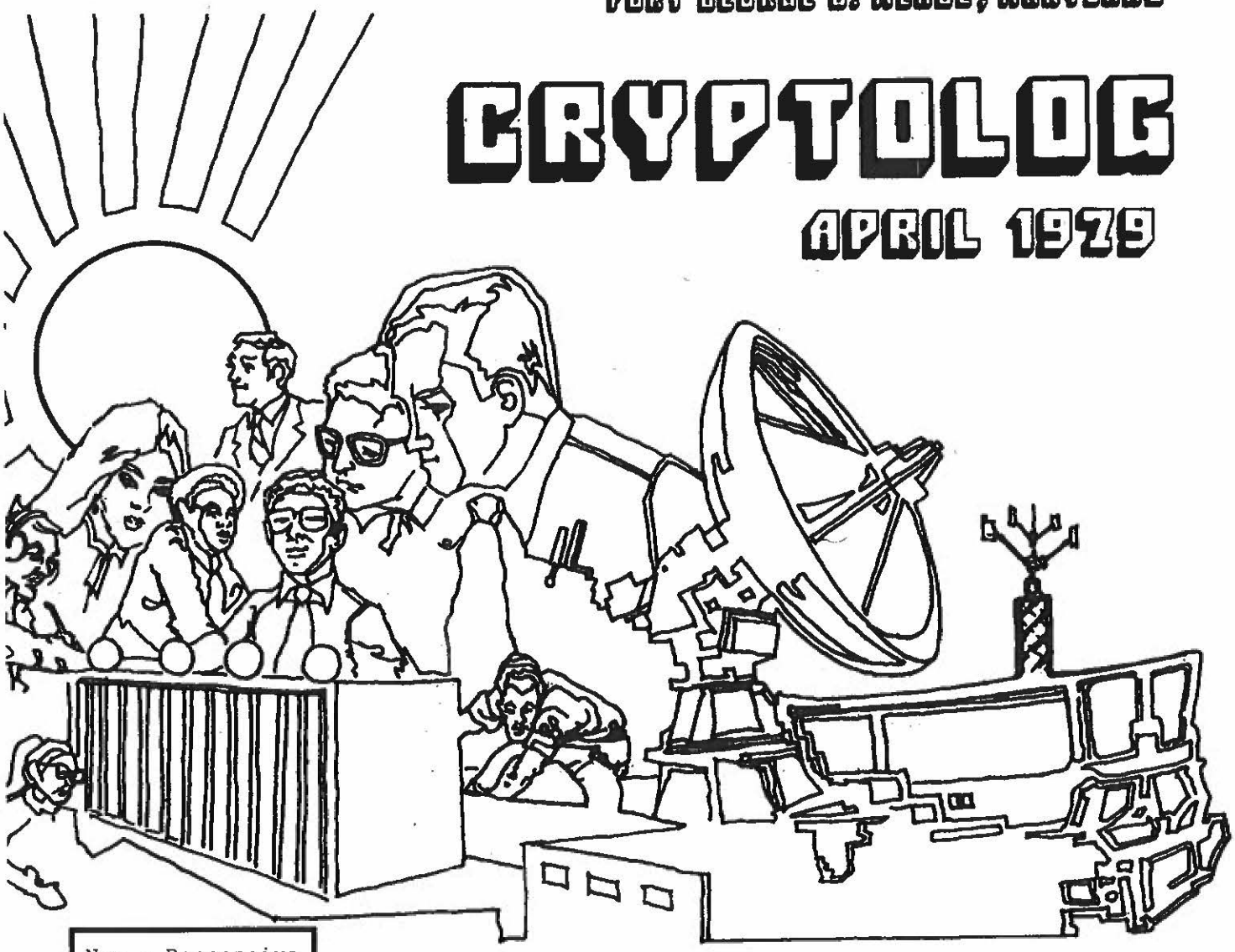
[redacted]

~~SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

APRIL 1979



Non - Responsive

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2
REVIEW ON 1 APRIL 2000~~

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,

for the Personnel of Operations

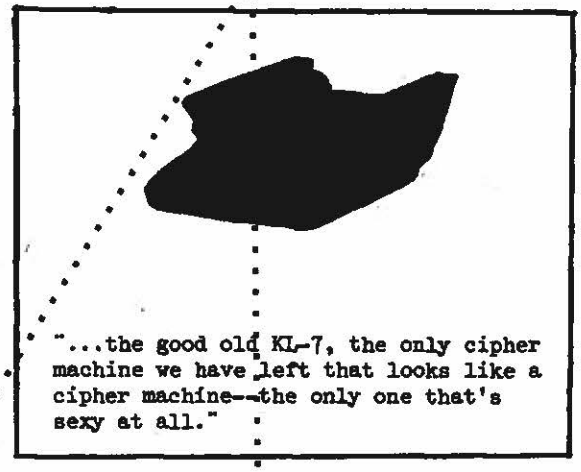
VOL. VI, No. 4 APRIL 1979

Non - Responsive

COMSEC/SIGINT Relations (U)

David G. Boak, S

Last November, David Boak, Special Assistant to the Deputy Director for Communications Security, NSA, presented an address on the status of COMSEC today to the members of the Communications Analysis Association. CRYPTOLOG *is pleased to be able to pass Mr. Boak's observations on to a wider audience.*



"...the good old KL-7, the only cipher machine we have left that looks like a cipher machine--the only one that's sexy at all."

(U) The easiest way to describe COMSEC is to say that it counters SIGINT. Our job in S is to frustrate the SIGINT professionals in hostile governments. Another way of looking at COMSEC; perhaps a more positive one, is to answer the question, "What's it for?" In a nutshell, I think that what COMSEC is for is to help the government achieve surprise. Now, I don't just mean the classical military tactical and strategic surprise, although, of course, that's crucial—but technological and diplomatic surprise as well.

(S-CCO) I believe that the SIGINT element of the national intelligence community remains the pre-eminent one. And the reason I do is that SIGINT provides to our decision makers the most timely, most authoritative, most accurate (and often unique) information those decision makers get about what the other guy is going to do before he does it. And that's equally important for a company commander, someone negotiating [redacted] position, a weapons system planner, or—increasingly often these days—someone involved in worldwide economic warfare. Denying comparable foreknowledge is what COMSEC is for. There are a few examples where we can demonstrate that a modest handful of COMSEC devices saved tens of millions of dollars in support of big operations, and some dismal instances in which we can show that the lack of COMSEC cost many lives. I suggest, therefore, that it is an excellent investment.

(U) Now, let's see what we're up against in trying to do that job.

(S-CCO) *The Threat.* Until the early 1970s this Agency had no coherent, comprehensive picture of what COMSEC was up against. We had fragmentary information. We got some of it from the SIGINT world and some from other sources. But, by and large, it was catch-as-catch-can. We assumed the worst about that threat and did the best we could to cope with it in an unstructured way.

(S-CCO) But we began to realize that our COMSEC assets were finite and that we had to allocate the resources, people, and machinery, as well as new developments, to optimize our position against the threat. And the better we could define it, the better we could get the right systems to the places where we were hurting the most. Therefore, we built an entire division with a specific mission of determining what we're up against, helping us assess what that meant to us, helping with our plans and our prioritizations. We could then begin to allocate such assets as we had on an educated basis.

(S-CCO) Here's a brief overview of what that group has developed as a picture of the dominant threat we face—

250 of those are in R. R1 is our heart and soul for the invention and the initial design of all the crypto equipment we build for the government. The balance, 1550 or so people, are in S. S and R1 act as friendly adversaries, with R inventing what we are going to use and our own S

S.

(U) At the core of all these people is a set of highly professional disciplines, notably cryptomathematics, engineering, and computer science. The SIGINT-oriented reader will note that, except for linguists, we are competing for and using the same kinds of key personnel resources.

(U) Cryptomathematics is obviously the heart of the whole assessment process for modern cryptosystems; I'll get back to them shortly.

Our need for engineers, particularly electronic engineers, is obvious. They are responsible for putting out cipher machines, the best in the world, literally in tens of thousands of copies.

We need computer scientists for at least three reasons. The first, and perhaps not so obvious one, is that every modern key generator cipher machine that we've fielded since the late 1950s can be viewed as not much more than a special purpose, hard-wired computer with some programability or variability to permit setup and change of keys. An understanding of the computer process is essential to the design and evaluation of the systems themselves.

(U) Secondly, computers turn out to be second only to brains in their importance to us as tools in the analytic process, and we use them extensively for that purpose.

And finally, in support of the cryptosystems we have worldwide is an enormous body of keying material, literally mountains of it, which in fact, has at its base computer generation. And we have a computer essentially dedicated to just doing that job.

Now what actually do all these brains produce? Let's have a quick look at our product line, the cipher machines we've already got.

The Response. What have we got ranged against these threats? Our COMSEC manpower is about eighteen hundred all told. About

One system, the good old KL-7, bears special mention for two reasons. First of all, it's the only one we have left that looks like a cipher machine; it's the only one that's sexy at all. All the others are just plain boring to look at. More importantly, the design for this crystalized in 1948. It got fielded in 1954 in some 25,000 copies. This old bear is still in use today, and we don't intend to phase it out until 1983. We expect the last message enciphered by that machine will remain secure against hostile cryptanalysis for five to ten years after that.

This is a prime example of the tremendous longevity of some of our machines. I point it out because I feel it justifies the highly conservative standards that we have imposed for acceptance of any high grade cipher machine. No changes have been made in the logic of the KL-7 since its inception, and we still think it is invulnerable to cryptanalysis without knowledge of its keys, rotor wirings or stepping patterns.

An examination of other, newer machines shows them to be progressively smaller, faster and more efficient. They include specialized highly reliable equipment for use in space. Some of these little boxes may cost as much as $40,000 a copy. That's kind of expensive. But then the first secure voice devices built cost a cool one million dollars each. So we're getting somewhere in keeping costs down. Also coming down the pike, probably our ultimate so far in

To support all these machines, we have a large organization putting out keying materials and many codes and manual ciphers as well. To get an idea of the magnitude of the operation,

I've mentioned 1800 or so people, some great technical specialties, a bunch of cipher machines, and countless manual systems. What do they do for us? How do they stack up against that rather awesome capability described earlier?

To appraise our posture, think of yourself for a moment as a member of a foreign SIGINT organization. You've been assigned to the job of exploiting U.S. communications. I'm going

Many of you have used the KY-3 Autosevocom system. Perhaps you don't know that when you pick up that phone to make a call, it automatically checks every critical alarm circuit in the system. If there's any failure that can jeopardize security, the system shuts down and you can't complete the call. It does that in the matter of a few milliseconds.

Our ultimate in alarm philosophy is perhaps the KW-37 used in the U.S. Navy's FOXTROT broadcast system. Here we use a transmitter with three identical key generators. All are set up, keyed and started simultaneously, and all three generator outputs are matched against each other. Unless at least two of these streams match exactly, the system shuts down. The third one can then be pulled out, fixed, and put back in without interrupting communications.

[redacted]

machines in the field from switches or net control stations

[redacted]

(U) Unlike the SIGINT world, we have a closed system. When we get done with stuff we destroy it, usually [redacted] So we don't have the problem with our product that you have with yours, of sending out dozens or hundreds of copies and having them merged, massaged, redisseminated, and then filed for months or years afterwards, vulnerable all that time.

[redacted]

scares us even more. So much so, in fact, that in the 1960s we began to say we've got to find some technical solution to this problem of the accessibility of our keys to better than 140,000 people. We came up with the concept of remote electronic keying where we could set up cipher

[redacted]

(U) Part of the difficulty, of course, is that communications keep growing. We keep being behind that power curve. It is estimated that the amount of communications in this country doubles every five years. Every time we start pumping out more cipher machines, communicators get more capacity, and we need still more cryptography.

(U) It's a very tough problem. The sheer magnitude of the requirement adds to the difficulty of finding cheap, effective, wide-spread voice security.

(U) Well, after a downer like that, let's see if there's a bright side.

(U) First of all, for record communications, virtually all are covered where classified traffic is involved. It's not a problem

PL 86-36/50 USC 3605

for us, and hasn't been for about 10 or 12 years.

[redacted]

(S-CCO) Physical security, apart from the remote electronic keying coming down the pike in our next generation of equipment, is advancing. We are improving the packaging of many of our keying materials to make them tamper-resistant, or to give us the means to detect the fact that someone in the pipeline has gotten at them. So we're making some progress there.

[redacted]

(S-CCO) Lying behind this is a tremendous infusion of money and effort—on the order of $1.3 billion over the next few years. That's big money for us, just for sheer procurement of hardware. That's about quadruple the expenditures we've ever made in a comparable time period before. As a result of this we are going to more than double our inventory by the mid-80s. Our estimate is that there are going to be over 500,000 cipher machines out there by 1985, if things continue to go as they're going now.

OK, let's get to the specifics of how we go about this job, how we evaluate these systems, get them out, and learn about our enemies. One key to the effort is the kind of interaction that has been going on in this Agency between COMSEC and SIGINT. Our association is a symbiotic one, with two separate organisms living in close harmony and interdependence, with each producing something the other can use to the mutual benefit of both.

[redacted]

(S-CCO) I think that among the biggest overall security contributions that the SIGINT community has made to the government as a whole in the last decade was the SIGINT discovery of North Vietnamese foreknowledge of USAF ARCLIGHT B-52 raids.

(S-CCO) SIGINT illuminated a tipoff net which was passing warnings, well in advance, of when and where these strikes would be made. It was good, strong, hard evidence which was then used for briefings in the Pentagon, to the JCS and DIA, as a result of which the first operations security (OPSEC) organization in our government was established.

(S-CCO) The Pentagon actually shook loose, like pulling hen's teeth, some 22 billets for the CINCPAC staff, including some senior people from our own Agency to go out there and carry out this OPSEC methodology. It involved looking at the security envelope around all our operations, seeing where the holes were, and plugging them. I suggest that, in the course of that war, it was one of the few bright spots in an otherwise dismal security record.**

(S-CCO) The methodology was great. It enhanced operations out there; it saved equipment and ordnance; it saved lives. It impressed the JCS so much that they established their own OPSEC organization; most of the other CINCs did likewise. Now all the services are using this technique, and OPSEC is a common word. In fact, we have a modest OPSEC capability in NSA itself, which I'll mention shortly.

(S-CCO) The SIGINT side of the Agency also helps us through sharing of assets, particularly computers. We could not afford the vast array [redacted] for COMSEC alone. But we use them continuously, and without them I don't believe we could reach the level of professionalism that we have [redacted]

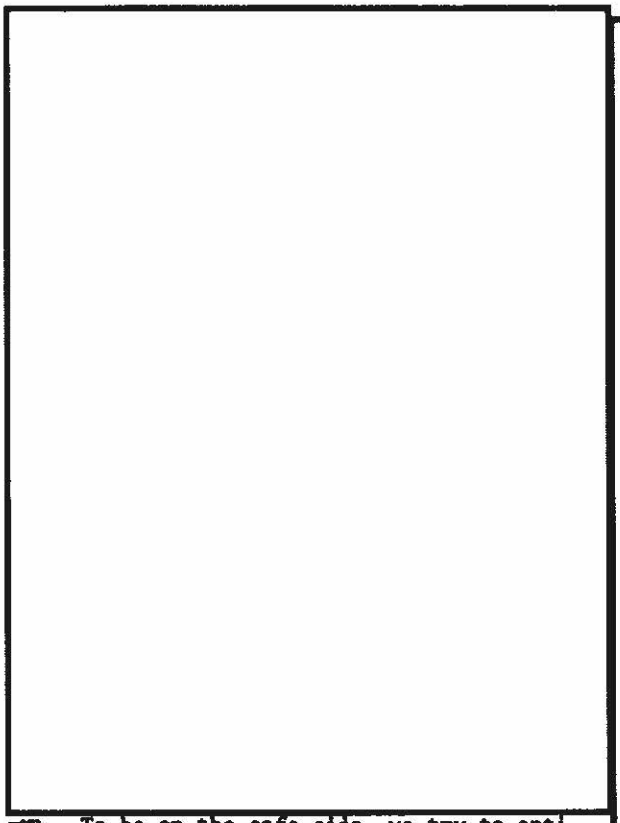
[redacted]

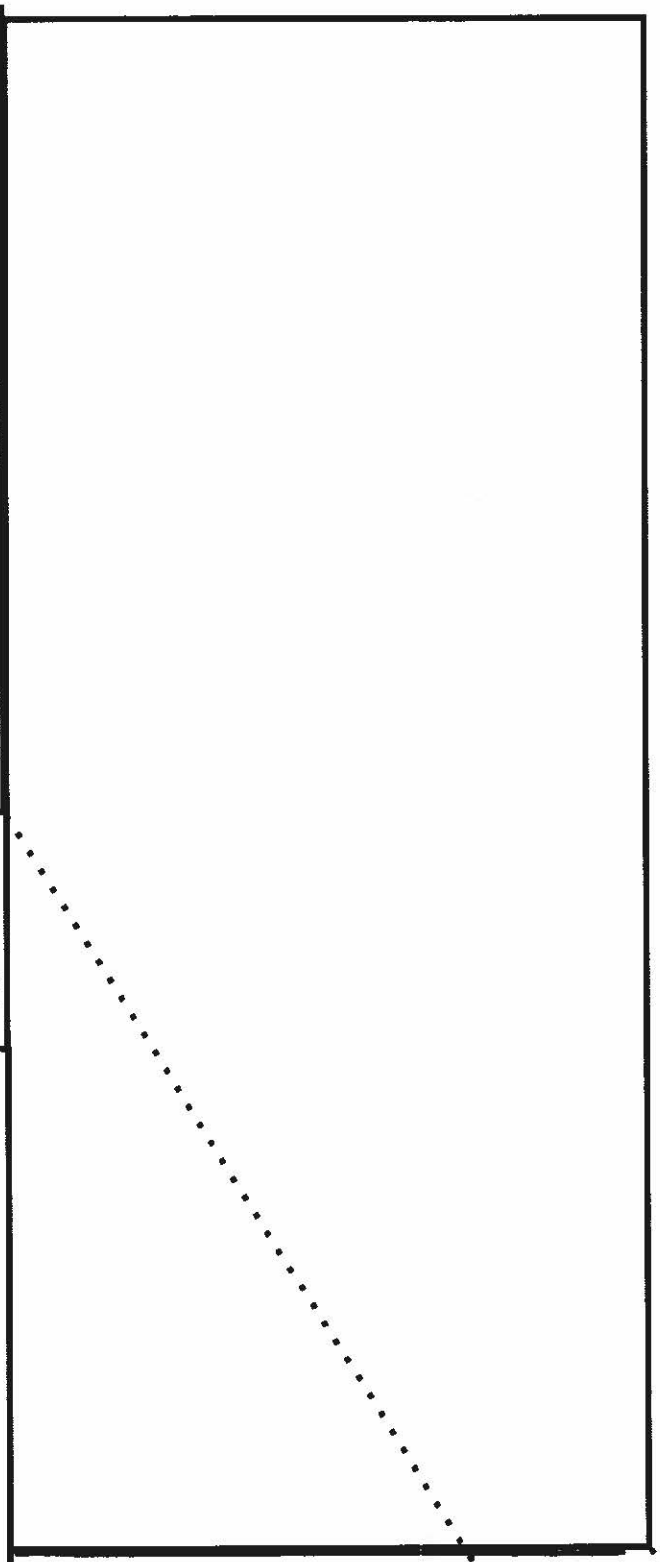
* For a related article see "Pursuit of the [redacted] in CRYPTOLOG, March 1979.

** One of the most dismaying aspects of this situation was that of the [redacted] operations examined throughout that theater, fully two-thirds—perhaps as many as three-fourths—of all the foreknowledge indicators that the enemy were getting were from our own communications insecurities.

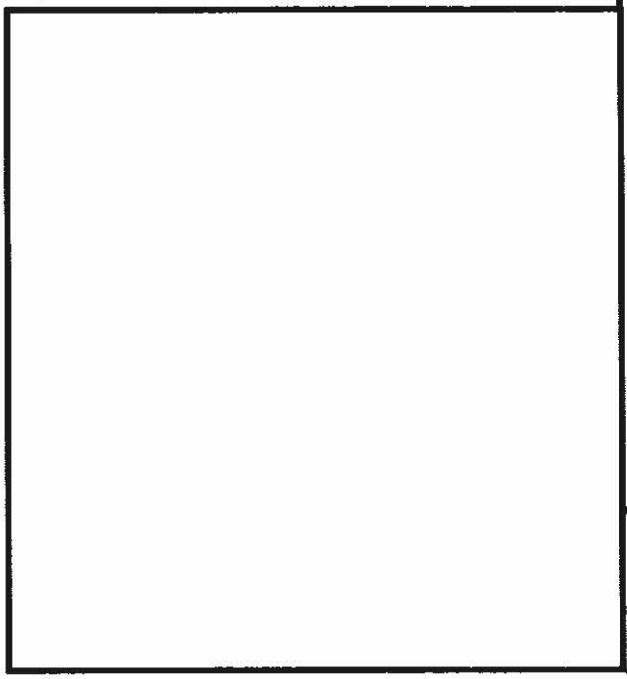
EO 3.3b(3)
PL 86-36/50 USC 3605

EO 3.3b(3)
PL 86-36/50 USC 3605





To be on the safe side, we try to anticipate future crypto-mathematical breakthroughs and accommodate possible jumps in computer power and still have a margin of safety. NSA is an image of what we think an enemy might look like if he's good enough. A knowledge of NSA's capabilities and procedures helps us in deciding how high to set our standards.



(Continued on page 18)

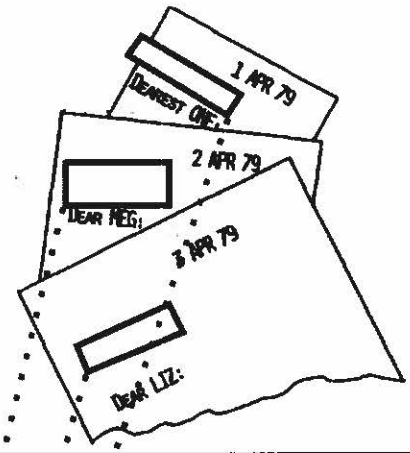
EO 3.3b(3)
PL 86-36/50 USC 3605

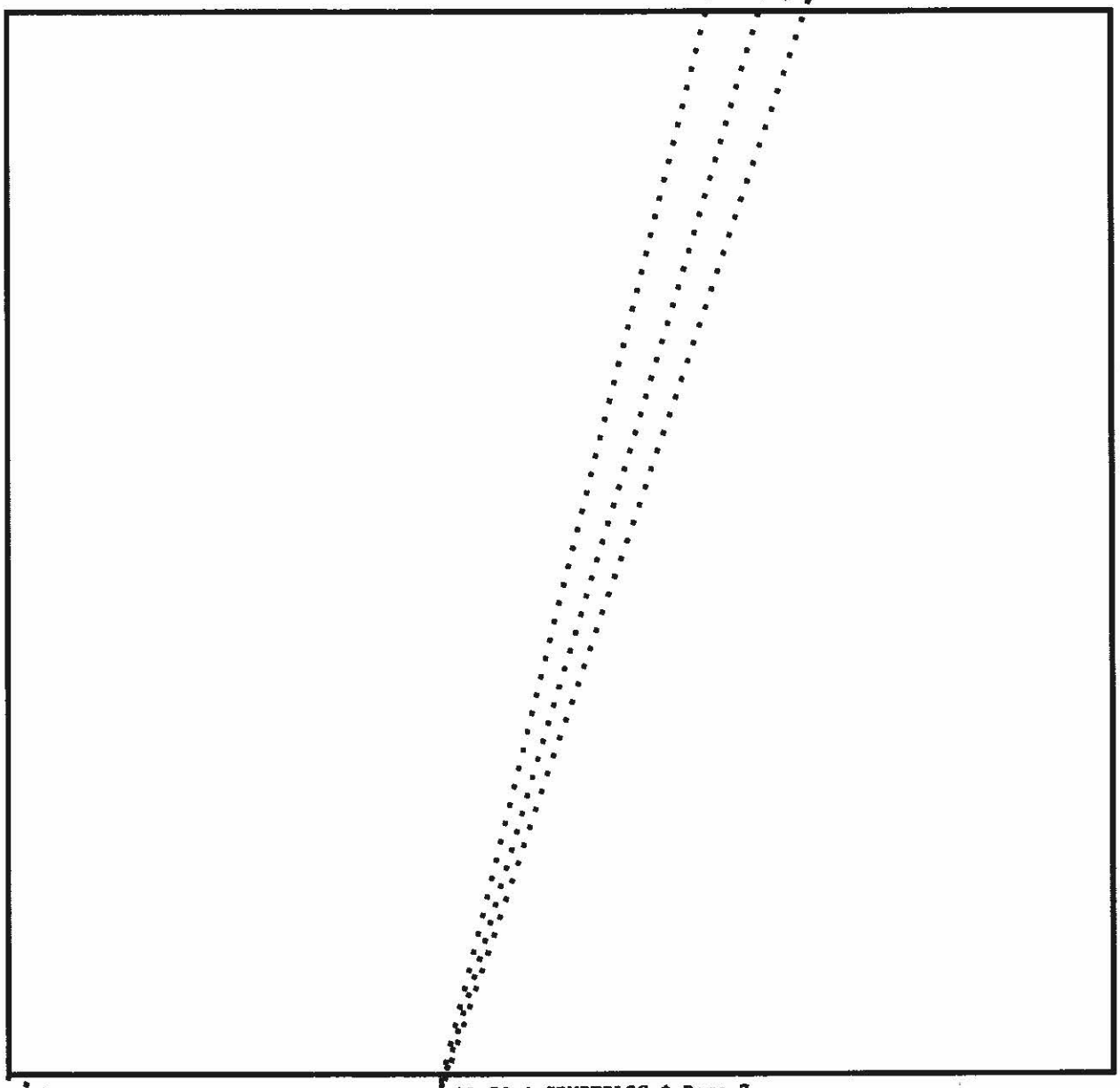
EO 3.3b(3)
PL 86-36/50 USC 3605

A Logical Sequel to "A Small Problem"
(CRYPTOLOG, *November 1978*)

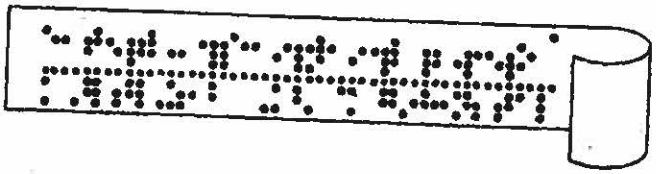
A Somewhat Larger Problem (U)

By Wayne E. Stoffel, P14
For the Crypto-Traffic Analytic
Special Interest Group



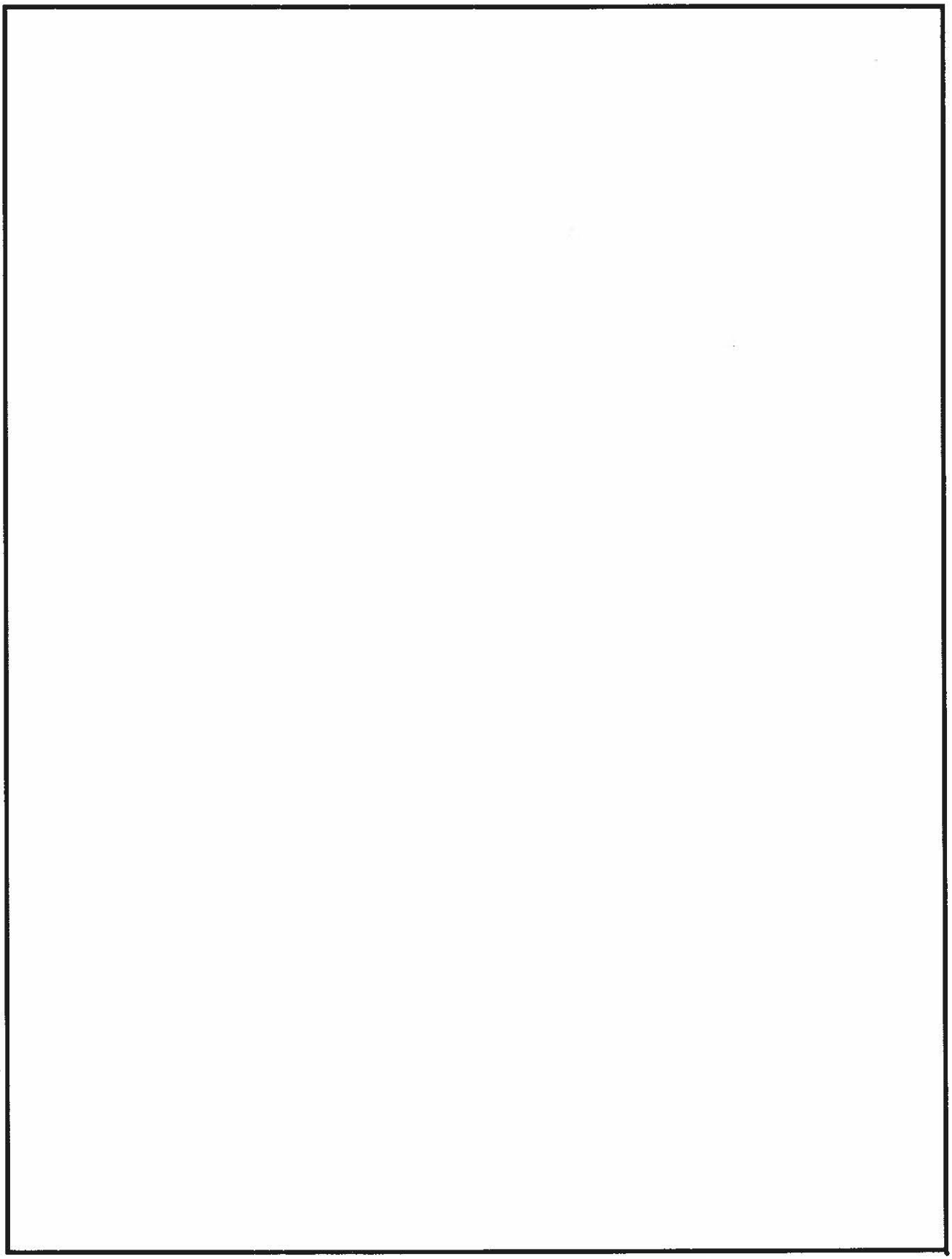


CLASSIC CABLES (U)

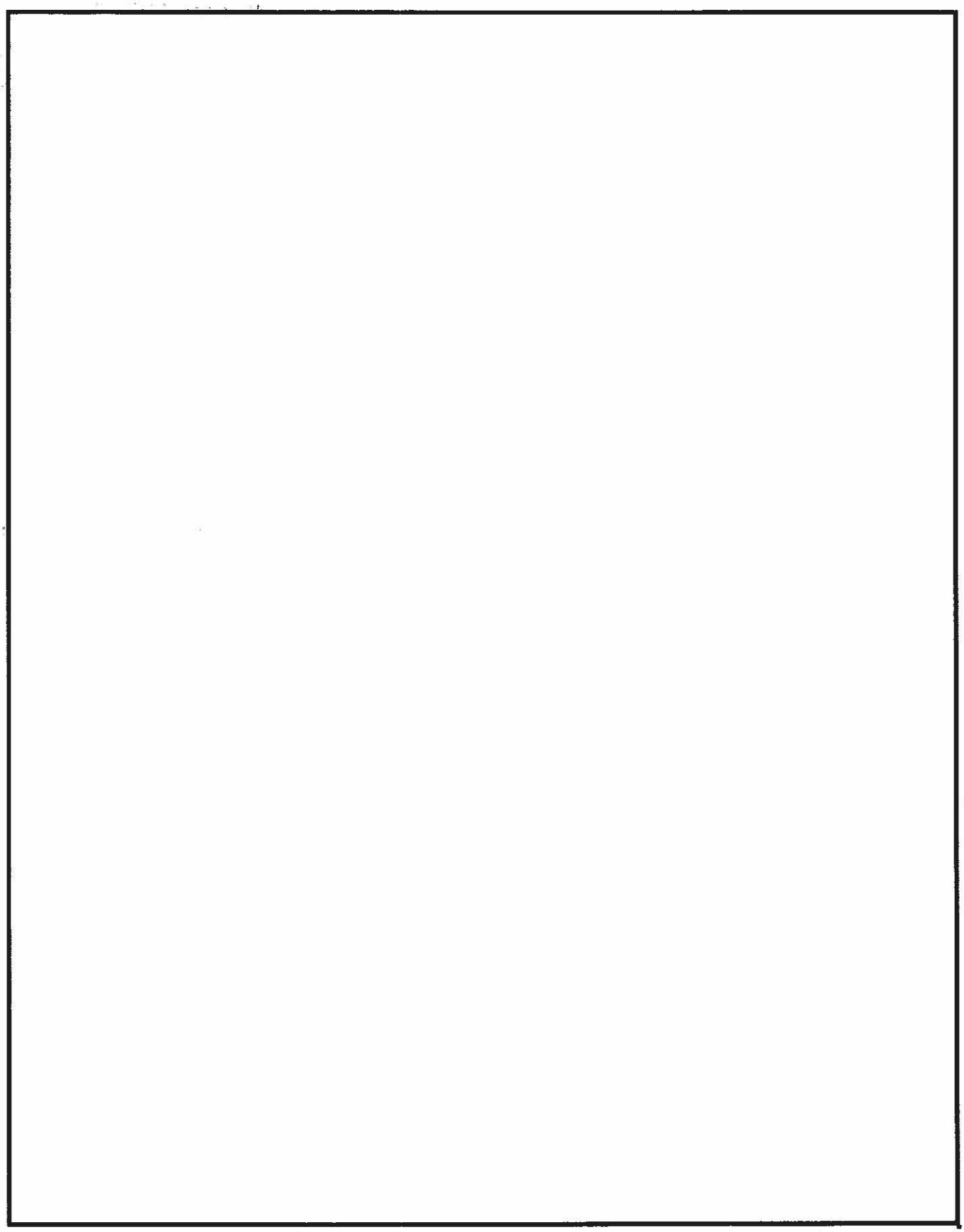


Not as well-known, perhaps, as Murphy's Law, but no less valid, is Hill's Axiom of Cable Analysis: *The exasperation of the cable drafter is directly proportional to the number of reference messages cited.*

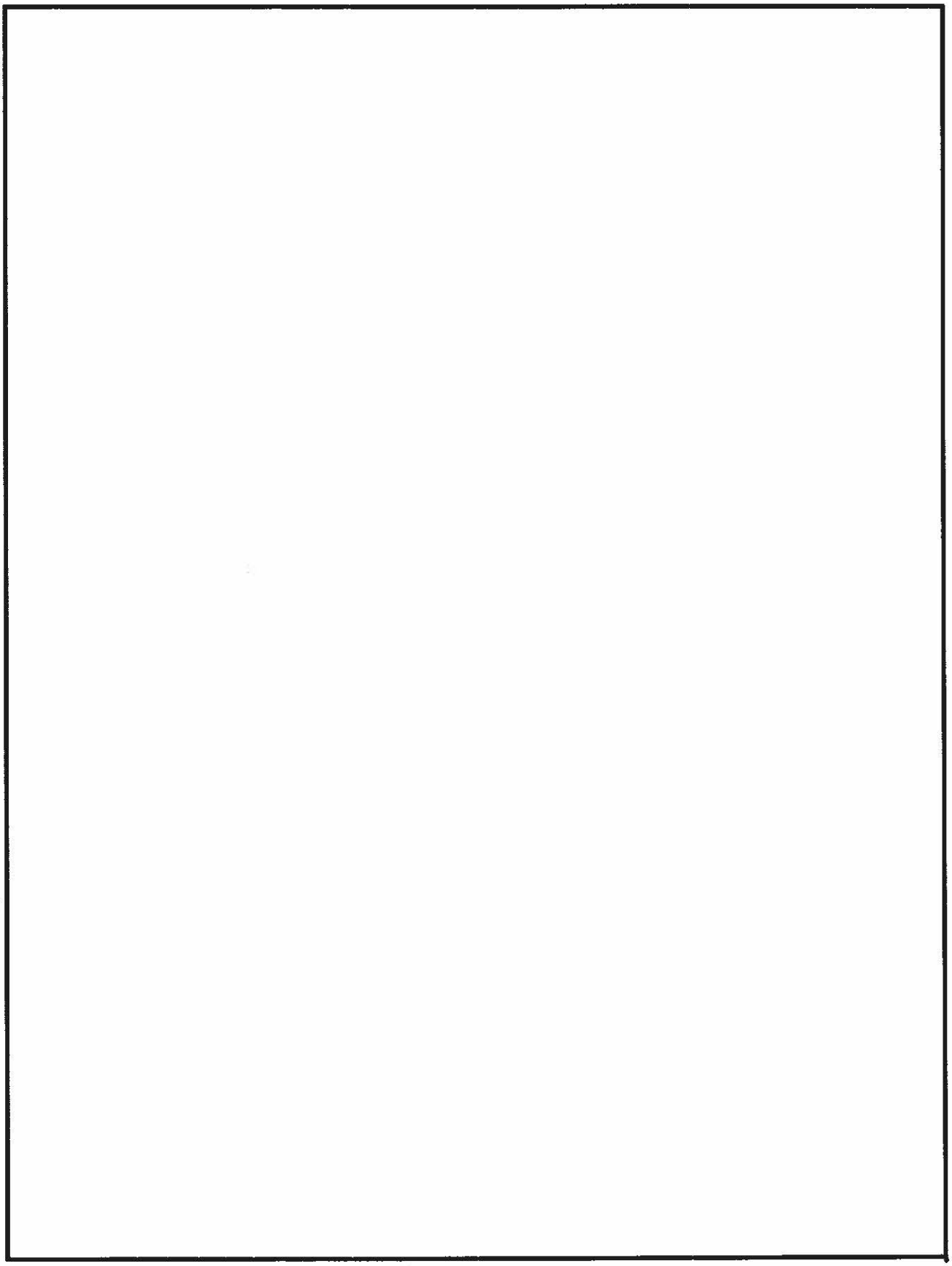
EO 3.3b(3)
PL 86-36/50 USC 3605



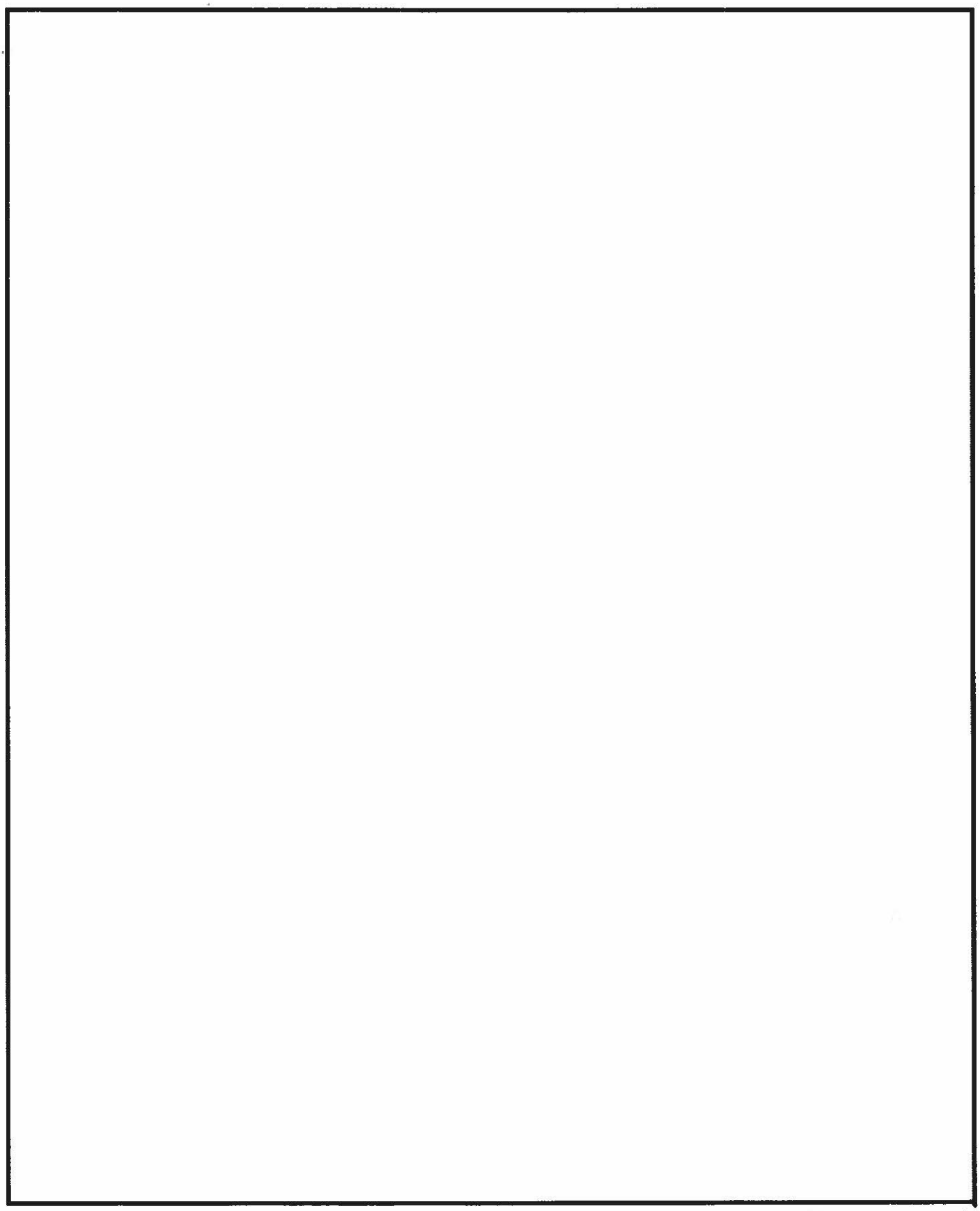
Non - Responsive



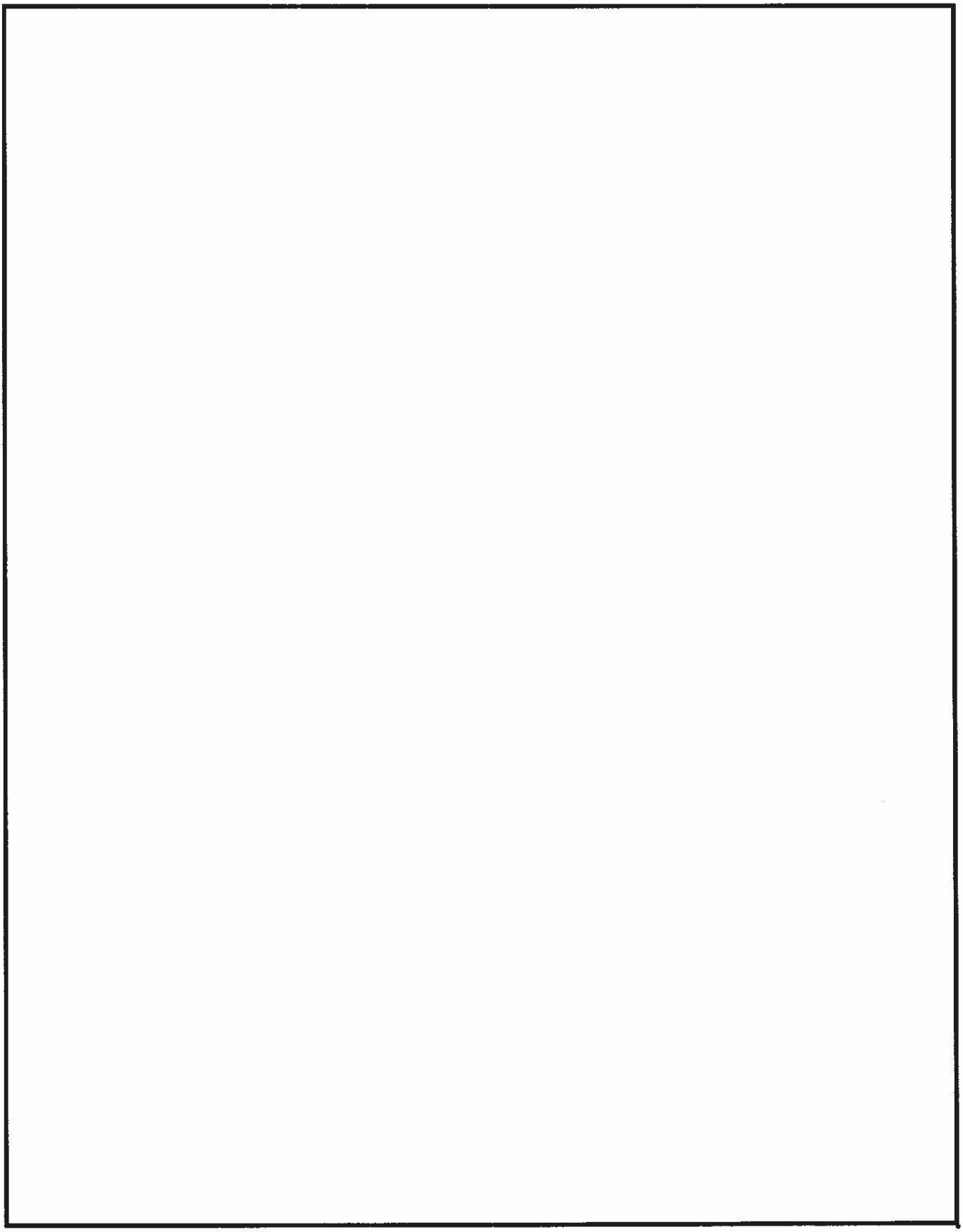
Non - Responsive



Non - Responsive



Non - Responsive



Non - Responsive

NSA-crostic No. 24 (U)

By D.H.W.

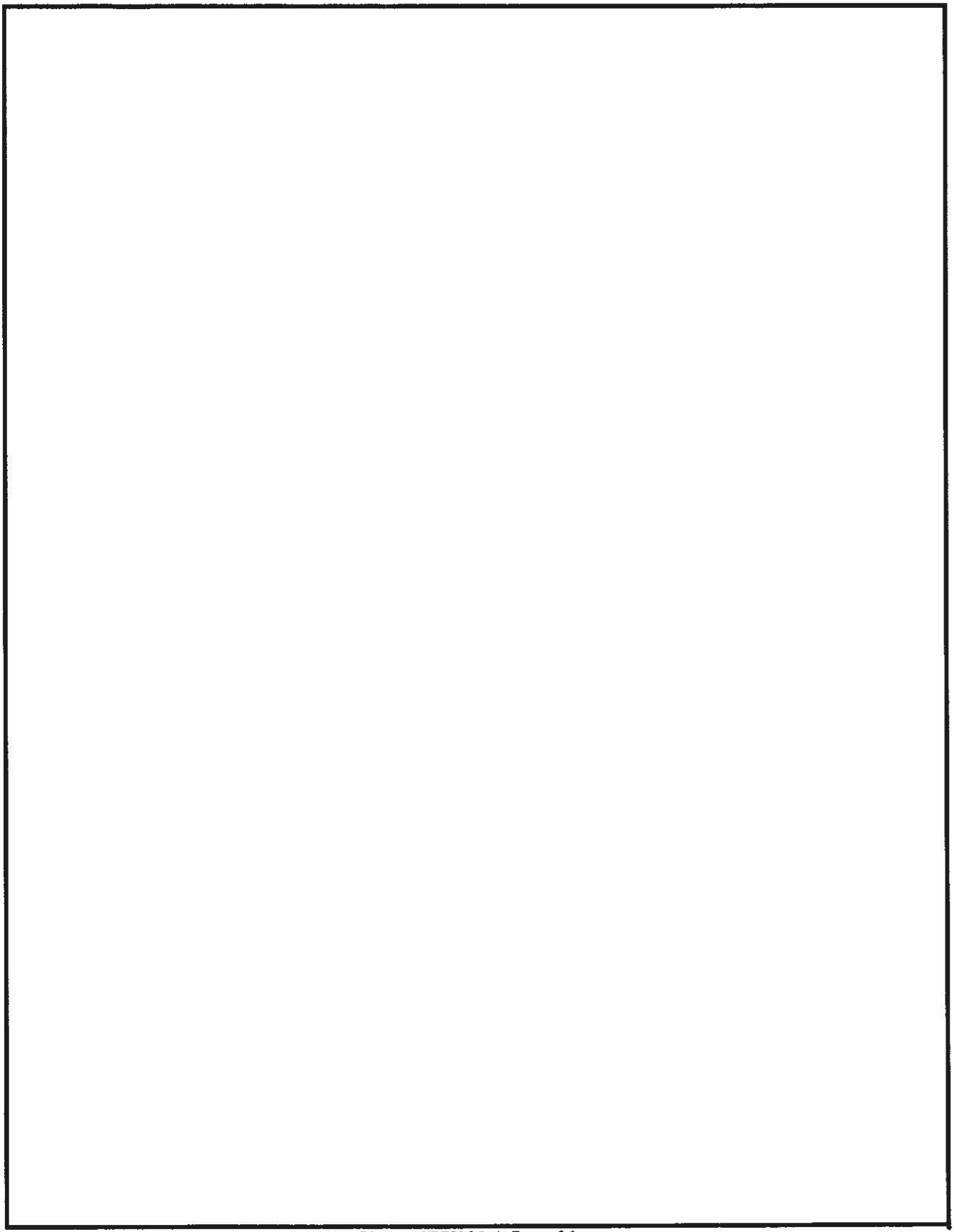
The quotation on the next page was taken from a published work of an NSA-er. The first letters of the WORDS spell out the author's name and the title of the work.

DEFINITIONS

WORDS

1 C	2 Z_1	3 J		4 G	5 D	6 A	7 R		8 N	9 X	10 Z		11 E	12 M		13 B	14 G	15 J	16 D
17 N	18 T	19 L	20 K		21 V		22 G	23 K	24 N	25 U	26 D	27 S	28 B		29 G	30 O	31 D	32 X	33 J
34 N	35 K		36 L	37 A		38 F		39 K	40 G	41 L	42 U	43 D	44 N	45 O		46 M	47 K	48 N	49 B
50 D	51 G	52 U	53 O		54 Z	55 V		56 E	57 F		58 K	59 B	60 N	61 X	62 T	63 O	64 J		65 M
66 C	67 R		68 L	69 B	70 O	71 T	72 N	73 J	74 C		75 W	76 G	77 T	78 S	79 C	80 B	81 N		82 S
83 O	84 P	85 D	86 T	87 B		88 I	89 C	90 N	91 B	92 T	93 M	94 X		95 L	96 O	97 V		98 Q	99 G
100 D	101 U	102 X	103 R	104 N		105 T	106 L	107 K	108 W	109 G	110 J	111 R		112 R	113 W		114 G	115 J	116 D
117 X	118 P	119 I	120 L	121 Q	122 N	—	123 J	124 H	125 N	126 K	127 V	128 X		129 B	130 W		131 A	132 Y	133 B
134 D	135 X	136 N	137 I	138 K		139 I	140 V		141 P		142 W	143 C	144 P	145 T	—	146 C	147 F	—	148 M
149 R	150 Z	151 T	152 I	—	153 W	154 Q	155 I		156 U	157 O	158 Q	159 H	160 E		161 F	162 T	163 I		164 E
165 A	166 N	167 U	168 D	169 J	170 P		171 Z	172 B	173 K	174 S	175 G	176 N	177 D	178 J		179 H	180 U	181 J	182 Z
183 N	184 B	185 X	186 Y	187 G		188 V	189 R		190 Y		191 G	192 F	193 P	194 B	195 V	—	196 Y	197 F	—
198 M	199 H	200 O	201 S	202 N	—	203 N	204 V	205 Z		206 B	207 I	208 E	209 H	210 K		211 L	212 B	213 Z_1	214 N
215 K		216 D	217 T	218 Y	219 J		220 P	221 D	222 K	223 Z_1		224 A	225 H	226 G	227 B	228 D	229 N		230 K
231 M	232 L		233 I	234 O	235 Z	236 B	237 H		238 R	239 N	240 X	241 Q	242 C		243 R	244 K		245 O	246 V
	247 V	248 D	249 P		250 U	251 G	252 D	253 N	254 O	255 X		256 K	257 S	258 E	259 G	260 A	261 C	262 N	263 J

(Solution next month) D.H.W.



Non - Responsive

Non - Responsive

EO 3.3b(3)
PL 86-36/50 USC 3605

(Continued from page 6)

[redacted]

Finally, I did mention that we have an OPSEC capability. We've been using that capability in S on behalf of NSA fundamentally [redacted] We think that we have helped make [redacted] activities more secure [redacted]

One final thought. I think that in the last ten or fifteen years the most salutary thing that I've seen happen in terms of organizational relationships has been the growing trust between COMSEC and SIGINT. We used to be at arm's length, and that's not happening anymore. In fact, we have integrated into the COMSEC process more SIGINT professionals in the last six or seven years than in the entire history of this Agency. COMSEC belatedly came to realize that SIGINT people have some brains after all and could do COMSEC jobs well—and that has proven out. [redacted] S [redacted] I can only hope that the people of the SIGINT side share my perception that the benefits are reciprocal.

EO 3.3b(3)
PL 86-36/50 USC 3605

Following his talk, Mr. Boak answered questions from the floor. ~~(This portion is classified CONFIDENTIAL in entirety.)~~

Q. What about TEMPEST?

A. TEMPEST—which is the Agency's term to identify potentially compromising emanations from our own electronic equipment—is a matter that I feel is reasonably well in hand as a COMSEC problem, as far as our [redacted] SIGINT job harder, and take more people and other assets to sustain our present level of success. But the consensus I see is that the problem is not an insuperable one.

The ascendency of the Department of Commerce in this field resulted from a presidential directive which established *two* Executive Agents in the government for telecommunications protection: one which has to do with the protection of national security related information—this is NSA, acting for the Secretary of Defense, and one for the protection of information not related to national security—this is the Department of Commerce.

The action element in Commerce is a new organization, the National Telecommunications and Information Administration, with whom we are now in active negotiation on how to share this load. We have some concerns, of course. Are they, for example going to create an independent cryptanalytic organization? Are they going to do independent R & D in cryptography? And if so, under what kinds of security controls?

Overall, however, we are becoming acclimated to one another and the Director is ensuring that we remain highly cooperative and supportive of them.

Q. What are your views on the extension of cryptography in the public sector and the initiatives of the Department of Commerce?

A. Frankly, I'm not overly concerned. I think some of us may have overreacted to the surge of activity out there and some of the publicity we got with respect to it. I think most of my SIGINT friends now believe that it is not going to be the end of the world. Clearly, though, as more and more sophisticated knowledge about cryptography is proliferated in public, it is going to make the

Q. Do you anticipate that the S organization will establish a viable ELINT security (ELSEC) program?

A. We have wrestled with that matter for as long as I've been around. We have not solved it. For a while, we thought of calling ourselves "SIGSEC" instead of COMSEC, thus solving the issue with improved nomenclature.

EO 3.3b(3)
PL 86-36/50 USC 3605

But it is true that we have no coherent ELSEC effort because we have been unable to define it very well. Yet those definitions are important in establishing roles, missions and authorities. The Army, for example, used to call telemetry a non-communications signal, and referred to its protection as ELSEC—a part of electronic warfare—and not within NSA's jurisdiction. We've largely solved that particular issue, but have not yet gotten a handle on how or whether to get involved in things like [redacted] What we have tried to insist on, though, is that, if a cryptographic technique is involved, regardless of the purpose of the signal, we should be in the act. But I'm afraid that's not really a very satisfactory answer.

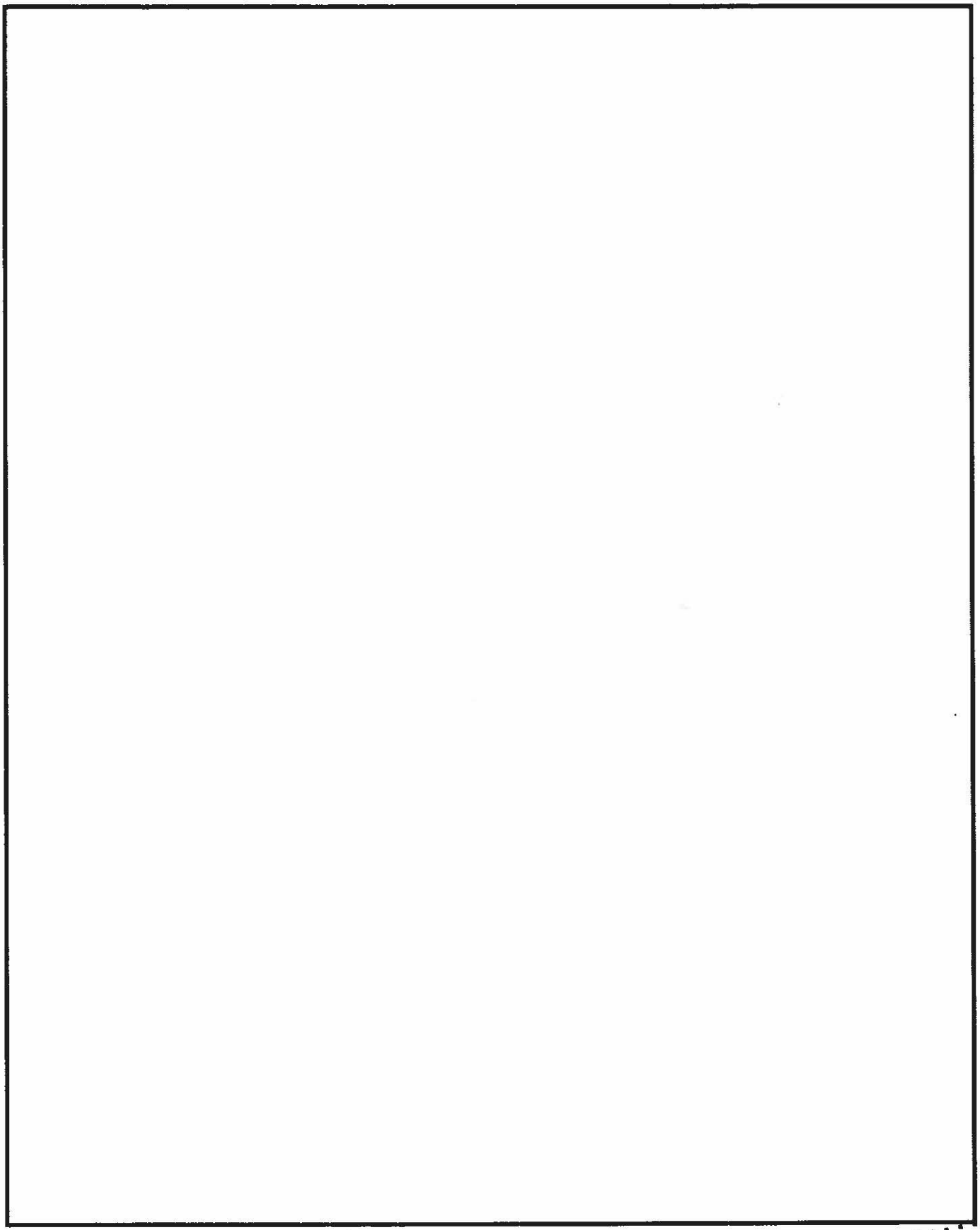
Q. Will NSA establish a national COMSEC assessment program for equipment other than that we build ourselves?

A. I hope not. It's a very difficult thing. If some of the equipment being produced commercially is going to be adopted by elements of the government, I believe we must have some role in its certification or validation. But I believe the way we go about that, if the equipment is not to be used for national security purposes, will have to be through the Department of Commerce, as their new mission gives them jurisdiction over such applications. We will offer them technical advice and assistance on how good such systems are.

Q. We seem to be with computer security where we were with TEMPEST ten years ago. What are your thoughts on where we are going in that area?

[redacted]

[redacted]



Non - Responsive

Non - Responsive