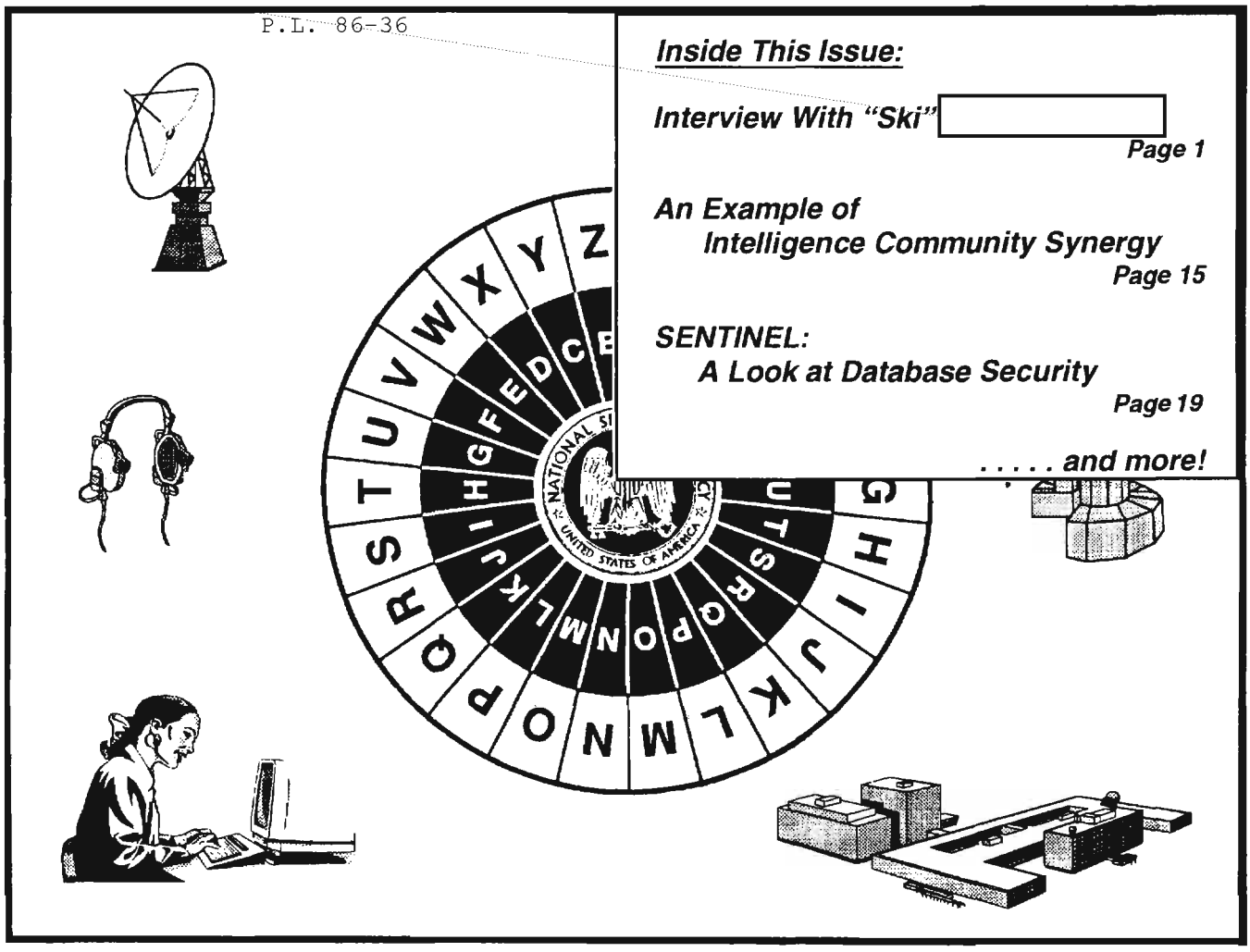
NATIONAL SECURITY AGENCY

CRYPTOLOG

The Journal of Technical Health

Vol. XXIII, No. 2 SUMMER 1997



Inside This Issue:

CRYPTOLOG

Summer 1997
Vol. XXIII, No. 2

Published by P02, Operations Directorate Intelligence Staff

To submit articles and letters, please see last page.

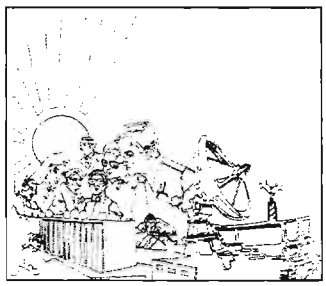


Table of Contents

P.L. 86-36

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

Perspective:

Lessons Learned

Interview with [redacted]

P.L. 86-36

One of the pioneers of signals analysis reflects on a fifty-year career in cryptologic service

(U) An important theme in Twentieth Century Cryptology is its expansion beyond the classic "code making and code breaking" endeavors that stretch back as long, or so it seems, as humankind has been attempting to communicate.

(U) The development of traffic analysis remains one of the most significant of those expansions. The analytic effort to derive useful information from the externals of message traffic, in addition to or apart from success in reaching the underlying plaintext of the message contents, ranks as a defining event in cryptologic history Beyond its intelligence value, traffic analysis pointed to something fundamental about the cryptology of our time: the fundamental importance of understanding not just the content of communications and the means to hide those contents but of the systems and technologies that carried those communications.

(U) An obvious point? In retrospect, possibly. But the history of cryptology and of the agencies that practice it are largely told in the gap between the retrospective obvious and earlier conventional wisdoms. After the Second World War, signals analysis represented yet another potential extension of cryptologic activity. But was it truly cryptologic in nature? Or was it more simply a matter of communications research, with, it might be granted, some intelligence implications.

P.L. 86-36

(U) [redacted] (any number of NSA personnel might hesitate for a second on the full name before reaching recognition with "Oh, you mean 'Ski.'") has spent a career, a half-century at the center of the evolution of signals analysis. In December 1996, shortly before his retirement, Ski discussed his career with *Cryptolog*.

(U) **Let's start chronologically. You went into the Navy in 1946, when you were 18 years old.**

(U) I was still 17.

(U) **Were you drafted?**

(U) No. The draft was still on, but the Navy had a program—I guess all the services had something like this—called the Kiddy Cruise. If you enlisted in the Navy at 17 and stayed until you were 21, you got credit for four years of service plus all your GI Bill benefits for schooling, housing, and all those other things. So I enlisted in

August, I was 18 in October, stayed for three years and two months or whatever it was; I would have received credit for four years of federal service had I stayed in.

(U) **How did you get into cryptologic service? Was that just a decision by the guy at the recruit depot?**

(U) No. It happened somewhere between the time I enlisted and the time I got out of boot camp. I was one of fifteen selected to be sent from Great Lakes, Illinois, to Washington, D.C., for this strange training that nobody knew anything about. George Rocawich was another in that group. He became one of our premier traffic analysts and just retired a few years ago. There was another group that came from the San Diego recruiting center, and they lorded it over the rest of us that they had come by ship to the East Coast. We had come by train from Chicago, so they had sea duty, and we didn't.

(U) We arrived in D.C., reported to the Navy Department, and they said we were to take off for a few days and then to report to Nebraska Avenue, the Naval Security Station or U.S. Navy Communications Station Washington (CSAW) as it was known then.

(U) **What did you do after reporting there?**

(U) The first thing, while we waited for our clearances, we were assigned in an LIC area in the attic studying electricity, math, typing, and cryptography. Our CO was CDR John Quincy Adams III, a direct descendant of President Adams.

(U) Jim Bates was part of that group and we always went to him with our crypt problems because he always had the solution first. From there, my first assignment after being cleared was in the personnel office. Then I was assigned to R&D, and I was a yeoman for a while and then communications technician or CT. From there I was reassigned to what became the R&D signals analysis lab. It wasn't called that then, but that's basically what it was. The Navy organization was N33 (later to become AFSA 334).

(U) In fact, though, the basic mission of the lab was for support to engineers building equipment; the use of signals analytic results for intelligence production was really a secondary mission. But we did have different kinds of signals coming in and the types of questions that were being asked—what kind of signals were they? How did they look? What did we have to cope with them? Who was the user? I took a real interest in that, so in addition to doing the administrative duties for the office, I also began working on the signals and found that more interesting.

(U) **We've been in a period of downsizing the last few years. But that period immediately after the war must have been a tremendously difficult period.**

(U) When I transferred from the Navy to civilian life in 1949, it was only through intervention of the folks inside the building that I got on board. They were not hiring—certainly not clerks. I wasn't exactly in a critical skill.

(U) But the fact that I had learned something about signals analysis and was interested in pursuing that made the difference. The chief of the research element needed someone who fit my qualifications, and he hired me. The Lord was smiling at me all the way on that one.

(U) **You were hired as a clerk?**

(U) Yes. "Clerk, General" is what they called it at the time.

(U) **At what grade?**

(U) Then it was called CAF-4, at about $2700 per year. Which was only slightly more than I was making in the Navy.

(U) **Were you at Nebraska Avenue when AFSA was formed?**

(U) Yes. They called us all together, the whole complex, to the back of the loading dock of what I think was Building 4A, while they announced that we were now the Armed Forces Security Agency. It didn't mean a whole lot, and of course the ser-

vices weren't too keen on the idea.

(U) **How much did things change after that? Did the Army people start to show up at Nebraska Avenue and so on?**

(U) Oh yes. There was a big exchange of people. I left Nebraska Avenue and went over to Arlington Hall. Because of the new structure new opportunities were available. That's where we started signals analysis in the production organization. The first organization was AFSA 204. The research folks were, as I said, more interested in the subject from the point of view of building equipment. The production element was very small: an Army captain named Ron Schmidt, myself, and two maintenance technicians. And me.

(U) But that was the start of what became NSA W34, T16, and A5? The latter two were evolved from the processing efforts whereas W34 stayed with signals analysis.

(U) **When you look at that fact on your résumé "started the first signals analysis effort in the production organization," that's a rather striking statement. It's hard to realize there was ever a point where we didn't have a signals analysis effort.**

(U) Well, there was the effort in R/D, but not in operations.

(U) **Was that controversial? Were there people who fought that?**

~~(S-CCO)~~ Signals analysis was not well understood at that time. At first there was no duplication of effort since our mission was so totally different from that of R/D. It did cause some problems later until the two efforts were joined in 1972. To answer your question directly, it wasn't something we set out to do with some elaborate plan. In fact,

[redacted]

(U) When I was in R&D we were using wire recorders, and it almost forced you to take up smoking. The only way to splice the wire was to tie the two ends of the wire—which was always breaking—in a square knot, pull it tight, and fuse it with some kind of heat. Well with one hand on each end of the wire, there was no way to hold a soldering iron or a match, so we soon learned how to touch the wire with the end of a lighted cigarette.

~~(S-CCO)~~ We worked at this for several years, but the idea of signals analysis in PROD did not really catch [redacted] Every job I had, and every time I either got promoted or we reorganized, my job was described as either an engineering aide or communications specialist or something. It wasn't until about 1954 that we came up with signals analyst to describe what we did.

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

~~(S-CCO)~~ In 1958 we became a division. Admiral Tommy R. Kurtz, USN, was the Director for Production (PROD) when we started to work

[redacted]

[redacted]

[redacted]

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

(U) I didn't realize this at the time, because when you're a GS-12 working in the basement you don't get too involved in the politics of *any*thing. But the Navy was very jealous, but Adm. Kurtz was convinced this was a SIGINT challenge and NSA was going to handle it. and we did.

(U) **Did you ever think you were going to be transferred back to the Navy or something like that?**

(U) Not really. Of course, AFSA had its problems. But then we became NSA and things seemed to settle down a little. But we still had—beyond my pay grade and my interest—politics of one sort or another. At my level, we had work to do, and signals to analyze, so we didn't get involved in it.

P.L. 86-36

~~(S-CCO)~~ And we were able to get things done. With NSA's help, the Navy was able to build the [redacted] That was built and in place in about a year. It was one of the fastest projects I've ever seen. I'm almost positive that Charlie Gandy in R/D built the recognizer that went to the field to recognized this specific signal. The real secret part of the whole project wasn't that we could intercept the signal so much as it was the ability to DF it. And that was built into the system.

(U) **You mentioned politics. What about the politics within the building. Were the signals analysts accepted as part of the process?**

~~(S-CCO)~~ No. In fact, what was then GENS 2 was not too keen that we were working on the [redacted] and we weren't part of GENS. So we were more or less tolerated. It helped tremendously that we had Admiral Kurtz as chief of PROD supporting us. Not that he ignored GENS 2, but he paid a lot of attention to us. He'd come down into the basement, take off the jacket with all those ribbons on it and hang it on a chair, and say, "What do you have today, Ski?" He was a strong believer in teamwork and saw to it that it worked for us.

(U) We had a terrific team. There was about five of us. Vernon Franks was in the Navy. Bruce Russell was a civilian analyst. Another who made

chief later on was CT1 James Killeron, USN. Leroy Spiess was our contact in GENS. But what a team!

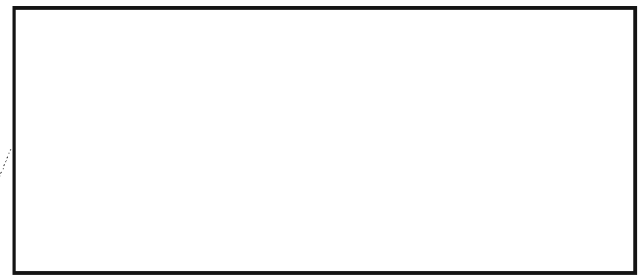
(U) I received the largest Special Act Award the agency had ever given to that time. Admiral Kurtz came down one day and told me he'd put me in for an award, and I told him I was going to have to buy him a coffee. "Coffee, hell," was his response. "You're going to have to buy me a car." That was a lot of money in 1960. But that wasn't the point. It was such a hard project, and so many people worked *so* hard on it. Not just at NSA, but the Navy, and the other services. It was a terrific effort. ADM Kurtz signed my picture of the presentation with 'team work with competence can't be beat.' That is still so true to this day.

(U) **Beyond cryptanalysis, beyond traffic analysis, the development of signals analysis could be thought of as almost another concentric circle of cryptology, couldn't it.**

(U) One thing that was different was that we didn't always pass things on from one stage of the process to another the way we do now. I had my job, which was signals analysis, and there was a sense that I didn't need to know whether the cryptanalysts were reading the system or not. We were much more inclined to say to the engineers, "Here are the parameters on which you need to work. Don't ask about anything beyond that." And we did the same with every other stage of the process. It was fairly segmented.

(U) **Talk about that. We are doing things differently, and there are very clear tradeoffs involved in that.**

(U) I think the way we're going now is a little better. I really do. I don't think everyone in the chain needs to know everything, but there were things we didn't know in the signals arena that folks watching the traffic did know. As it turned out, sometimes we found out things by accident that we had to know, such as the length of standard messages. We had to know that, and we have to be able to share information.

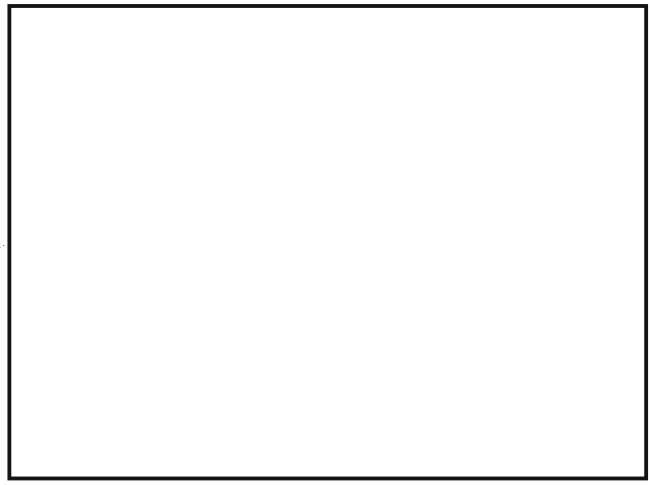


(U) It really helped to know schedules and things of that sort, so we would know where to look. We didn't have to know every detail.

(U) **Let's talk for a moment about career issues. Were you one of the early group to come out to NSA?**

(U) Not the first group, but early on. Some things haven't changed. We reorganized a lot, and people moved back and forth between Nebraska Avenue and Arlington Hall, and then we got ordered out here. It never failed. Every time I moved my residence to get closer to work, I got reassigned.

(U) **What was it like working for NSA in the 1950s?**



(U) It was just the best place to be. I guess that's what kept me here for fifty years.

(U) **But you get the sense—greater secrecy and all—that this was a much tighter community of people.**

(U) I was talking about this just the other day. You kept such a close hold on what your did and where you worked. You took your badge off when you cleared the gate. You told people you worked for the government or the Defense Department. If anyone asked what you did, you said you were an analyst, or an engineer, or whatever. A good example is that my Navy records do not reflect my assignment to CSAW, but merely to Navy Barracks Washington D.C.

(U) When I first saw the terms signals analysis and COMINT in the newspaper I nearly had a heart attack. ELINT was one thing, because the services had their own ELINT operations, and so on. But COMINT! That was enough to send shivers up my spine.

(U) **You really had an extraordinary group of folks at the top of the place, didn't you?**

~~(S-CCO)~~ The nice part of my job was it took me through all the different components of NSA. Dr. Tordella was actually the Chief of C at the time

[redacted]

~~(S-CCO)~~ Dr. Tordella had that ability to see the whole SIGINT process. And he was such a human person. I was standing out in front of the building one day when Dr. Tordella was escorting a senior DOD official out to his car. They walked past me, stopped, and turned around. Now, it was around 5:00 in the afternoon, so I didn't think I was leaving early. And even if I had, I didn't think Dr. Tordella would chew me out in front of a visitor. But he came over and told the visitor that I was the gentleman responsible for all the requests NSA was putting on the department of research and development as a result of all the new signals we were finding, [redacted] I was glad that was over, because I didn't know what he was going to do.

(U) His heart was really in the technical end of the business. He'd come down to the basement, look around, and ask questions. From time to time, he'd stick his head behind the racks to see how everything was wired up. And he didn't like to see wires just tossed around carelessly back there. He wanted them neat and laced together. He was one of the finest people this agency ever produced. Of course there are many others, but I think of him as certainly one of the best.

(U) **Like a lot of the people from that era, you had come in from the service, without a college degree and then ended up going to school at night.**

(U) That was very common in those days. And you'd go down to someplace like George Washington, and you'd find Dr. Tordella and people like that teaching a course and a number of your fellow workers in class with you.

(U) Working full time, going to school, sometimes holding a second job. It was tough. But those were good times, and I wouldn't trade them for anything.

(U) **You stayed in the signals analysis effort for a long time and then went off to field operations. What was that all about?**

(U) I went to the Air War College, graduating in 1968, and they wouldn't let me have my old job back. At the time, that was probably one of the bigger disappointments of my career. So I went to work in field operations. At that time, anything that involved feedback to the sites, making sure

they were properly equipped and informed went through there. We were basically responsible for seeing that they had what they needed to do their jobs.

(U) One of the problems we had was that all the group chiefs at that time, people like Art Levenson and Frank Raven, were going in to Gen. John Morrison, the DDO, and trying to get top priority for processing. So the folks in the processing area got a little tired of three and four people asking for some sort of change in priorities, all based on the idea they should have first shot.

(U) So, General Morrison decided he was tired of hearing all of this and decided we needed a plan. So, the Signals Processing Requirements Panel was born, in order to sort out some of this. It was staff work, pure and simple, which I wasn't too keen on, but it had to be done. I only spent a couple or three years there.

(U) Followed by a tour in the office of ELINT?

[redacted]

(U) So you've been a manager but always with signals analysis roots. How do you feel about the relationship between technical skills and managerial skills?

(U) From a personal standpoint, I had the best of both worlds. I knew enough from the technical side to hold my own in signals analysis and collection. I was not an engineer nor a mathematician, so if I tried to go back to signals analysis these days I wouldn't stand a chance. Somehow, along the way, I'd acquired enough managerial ability—I think I was good with people and good at pulling teams together. I don't know really how it happened. I went from being a section chief to a branch chief, to division and ended up being the deputy of W3. But because of my early background I was viewed by some folks as technical; others saw me as managerial. To this day, I still don't know how the decision was made to make me an SLE but I am certainly glad it was done!

(U) The fact is that in those days you didn't get ahead unless you were a manager. If I hadn't become a branch chief and a division chief, who knows where I would have ended up.

(U) And that's a continuing issue.

(U) I think at least through branch management, you have to have technical roots in this business. You have to have some sense of what your people are doing. You have to be able to mentor them and help them solve their technical problems.

(U) We're going to have to leave some details of your career to the oral history program. You've spent so long as Technical Director of B Group, I want to spend some time on that. How did you wind up there?

(U) I had spent seven years as Deputy of W3, the Office of Search. It was time for me to move. I was transferred and at the request of [redacted] was assigned to R5 to do a study of the signals analysis effort and to work on development of a system for moving technology out of the R labs into the operational areas. The signals analysis work force was aging and there were no people in the pipeline.

P.L. 86-36

(U) I was disappointed in leaving W3, and I was planning to make R5 my swan song. But when [redacted] announced he was going to private industry, I was determined to finish the study before he left. I finished the study and it became the basis of an R/D and DO implementation plan. And with that done, I was returned to DO, with a note from [redacted] saying they were sending me back unharmed. One day, [redacted] approached me and asked me to come back to B as tech advisor. During my first ten years in B Group I

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

had eight different chiefs. I've told people my job wasn't technical, my job was to train group chiefs and in fact had a sign that said, "Honk if you have been the chief of B!"

P.L. 86-36

(U) When [redacted] came in, he wanted to do what we would now call SRTD work, in one division for all of B. He wanted me to head the division. It was there that I was promoted to SLE. At the time the rules about how many people SLEs could supervise applied. And one day, Dick Lord asked [redacted] where I had been assigned, and when [redacted] told him, Lord said maybe they should take the promotion back. I quickly requested a vote in that, so I went back to being the tech advisor.

(U) Every one of the chiefs has used me differently, depending on what their strengths were. And where they felt there was work to be done.

[redacted]

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

~~(S-CCO)~~ So I was always able to stay close to the signals and have fun with that. My job was to keep management informed of the trends and new signals appearing. I often believe that I had two

[redacted]

(U) How did the change to the new B affect you?

(U) I had build up a good rapport with a lot of people in the old B, so I had that base. And I knew many of the people coming in as part of the new B. So that was a help.

(U) Beyond that, the chief, [redacted] was very interested in two projects: SRTD and the development of the technical track. Those duties became paramount, so I never got involved with the signals folks in the new organization the way I had before the reorganization. Most of my chores were involved in making the structure work, and working on details, and going to any number of working group, panel etc. meetings.

(U) One big part of my job has been convincing people that there is more to the tech track than books and trips. There is more to getting a title than just getting a title. There is a payback associated with this effort—payback to the mission as well as to the people you work with.

(U) We've gotten so big. Managers have gotten farther and farther away from their technical people. And here we have a chance—as signals analysts judging signals analysts or IA judging IAs—to say to management, "When you start thinking about promotions, here are our best people." It's not a hoop you jump through.

(U) Think about the professionalization program. I know people have mixed views about it now, but you have to recall its origins. In signals analysis, most of our people had come in from the military, without degrees, and we had very little with which to motivate them to continue their development. Professionalization forced them to keep up with things, to learn about things they might otherwise have neglected. And the technical track offers us the same opportunity.

(U) Too often we think of the technical track as something you need to get promoted. And it's not that. It's you as a person. It's what does Bill bring here, and what value do we put on his talents, and what training and experience do we give him to make him better. That's very important.

(U) Professionalization developed our specialties; the tech track seems to offer the prospect of integrating those specialties. Is that a fair way to put it?

(U) The pendulum swings back and forth on that. When I came in, signals analysts were to learn signals analysis, traffic analysts were to learn traffic analysis, and so on.

P.L. 86-36

(U) Then we seemed to want to spread out a bit more. But that can go too far as well. The Army has that slogan "Be all you can be" and I like that as a way of saying develop a skill that you can excel in. Not to the exclusion of everything else, but from a base in a skill that you can truly master. Of the three possibilities, that's the one I like best. I hope that's where we're heading.

(U) **As you look back over the last fifty years, what's your proudest accomplishment?**

(U) There's no question that I'm proudest of the signals analysis lab and getting to the point where its survival was assured. I still meet people who go back to that era and who are now long gone from here, but who see me and come up to say that the lab was the best part of their career. From a personal view, that's my biggest accomplishment. For the mission, I think that had a real impact. Without signals analysis, I don't know where we'd be. Today the skill fields are a bit less defined and signals analysis overlaps a number of others, such as cryptanalysis and engineering for example. But the signals analysis function remains a corner stone of the cryptologic family. Another area I am proud of is the SRTD effort, but the success of that effort remains to be graded.

(U) **You came in at a time of downsizing and transition. And here we are again, with a fair amount of concern expressed all around. But the lesson is you can do good work in those times.**

(U) Somehow you manage. Sure, you have things going on, you have things to worry about. But whenever there's been a crisis, this agency has turned to. Nobody raises the question of overtime or all that; nobody even thinks about being here all night in a crisis. Our people respond. They always have.

(U) **Any last thoughts?**

(U) It's going to be tough to leave. When I took my last polygraph, the operator was astonished to find I had been here fifty years. So, when he asked that sneaky question they always ask at the end, it turned out to be "In your fifty years here, have you ever been unhappy?" And I said no. I don't what the response was on the machine, but I owe this agency an awful lot. I really do. I'll always remember the people here. We have our ups and downs, but as far as the mission is concerned, as far as the sense of having contributed to what General Minihan described as avoiding "the war we didn't have," I feel like I did make a contribution.

(U) **At the Navy Memorial on Pennsylvania Avenue, there's a quote from President Kennedy to the effect that no man should have a prouder boast than that of having served in the United States Navy. You could make the same case, I think, for the Cold War American Intelligence Community.**

(U) I'm a plank owner of that memorial, and could never be prouder of my long association with both the U.S. Navy and the NSA. My thanks to both for a most rewarding opportunity.

KA

CRYPTOLOG
Summer 1997

Signals Analysis: The Untold Success Story

by [redacted]

The Background:

(U) After World War II, both the Army and Navy conducted SIGINT activities as independent efforts. The Army's effort was headquartered at Arlington Hall Station (AHS) in Virginia and the Navy on Nebraska Avenue in Washington, D.C., (CSAW). In 1946 the Navy's headquarters was also known as the Naval Security Station (NSS) and as Communications Station Activity (Washington). Captain Harper was the commanding officer.

~~(FOUO)~~ The Research and Development department was headed by Mr. E. N. Dingley, Jr., a captain in the U.S. Naval Reserve. A number of R&D positions were located both in the continental U.S. and overseas. [redacted] were charged with search and collection of new signals and the testing of new equipment to cope with the growing technology of the time.

(U) Signals from these collectors were sent to CSAW (I believe the designator at the time was N33). LCDR Fred W. Hitz, USN, was in charge of a number of senior civilian analysts/reporters who reported the findings, verified the analysis and did the tasking. Mr. James Cochrane, and Ms. Nancy Swann were assigned along with several other navy and civilian personnel. CTC Jack Ciska, USN, was the yeoman.

(U) The actual analysis of these signals was performed in N33 under the supervision of Mr. Russell L. Hoepner. The personnel either all Navy veterans or active-duty officers. Among the best were Mr. Edward J. Malone, Mr. Henry Stamps and CWO "Poochie" Jones, USN. I became a member of this team in October 1949.

(U) In late 1949 the military intelligence services (ASA, NSS and now the Air Force's AFSS) joined to become the Armed Forces Security Agency, at which time my organization was renumbered AFSA 334. By this time the volume of material requiring analysis was growing along with the need to process not only printer and time-multiplex systems but a very large input of facsimile. The volume processing of these signals from wire and disc recordings was fast becoming a problem for an organization more concerned with new technology.

(U) In mid-1951 a new organization, under the auspices of Captain Ronald Schmidt, USA,was being initiated at Arlington Hall Station as AFSA 204. The primary function was to do the processing and analysis from SIGINT stations worldwide. I transferred from AFSA 334 to AFSA 204 and, along with Mr. Schmidt and two Army sergeants (one of whose name was Arsenault), began the first signals analysis effort in the Production organization.

~~(S-CCO)~~ Beginning in 1951 the organization withstood a number of reorganizations caused by the increasing number of Soviet signals, processing demands and attempts to find the right fit for this still-misunderstood element. These growing demands also resulted in increased manning. Cap-

tain Schmidt became the civilian chief, Sergeant Richard Gibson, USA, and Mr. Joseph Marenick were added to the group. By this time the increase [redacted] Mr. Hoepner was added to the management team as we built a rather large processing facility in the basement of the cafeteria at AHS. As we grew out of our spaces it was decided to move us to NSS. By this time we had added additional people to perform signals analysis, the master being a retired Navy radioman named William Skinner. We had also divided the functions into processing and analysis, with Skinner the chief by virtue of his experience and talents.

(U) In May 1956 the signals analysis effort returned to AHS, but the processing remained at NSS. We were now COLL-331, soon changed to COLL-221. Eugene E. Embry was the chief of COLL-22 and Bill Skinner of COLL-221. We were assigned to COLL-2 because this was the technical arm of Production, much along the lines of the original Navy organization 334. In late 1956 we returned to NSS from whence we moved to Ft. George G. Meade in 1957. It was not until early 1957 that we were recognized as Signals Analysts by the Civil Service job descriptions. Until then we were Clerks (General), Engineering Aides (Electronic and/or General), Communications Analysts/Specialists and finally Signals Analysts.

~~(FOUO)~~ In February 1958, the signals analysis effort had grown to division size and I was named its first chief. In 1959, since COLL did more than Collection, the title was changed to COSA to reflect the Collection *and* Signals Analysis efforts. It was during this time frame that the extension of the signals analysis effort to the "front end" of the SIGINT system was made. [redacted] was established with Mr. Joseph Sausnock, Jr. assigned as the chief. Mr. Russell "Jose" Rogers performed the same function at the [redacted] Both of these men were ex-Navy personnel who had excellent training and were experienced signals analysts, and who had been section chiefs in COSA-34. From its humble beginnings at AHS, the Signals Analysis career field had taken its place among the best of the best in the intelligence business; J45, Z15 and W34 all trace their roots to AHS.

(U) I remained the chief until August 1967 when I was assigned to the Air War College, at which time Mr. George Jelen replaced me.

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

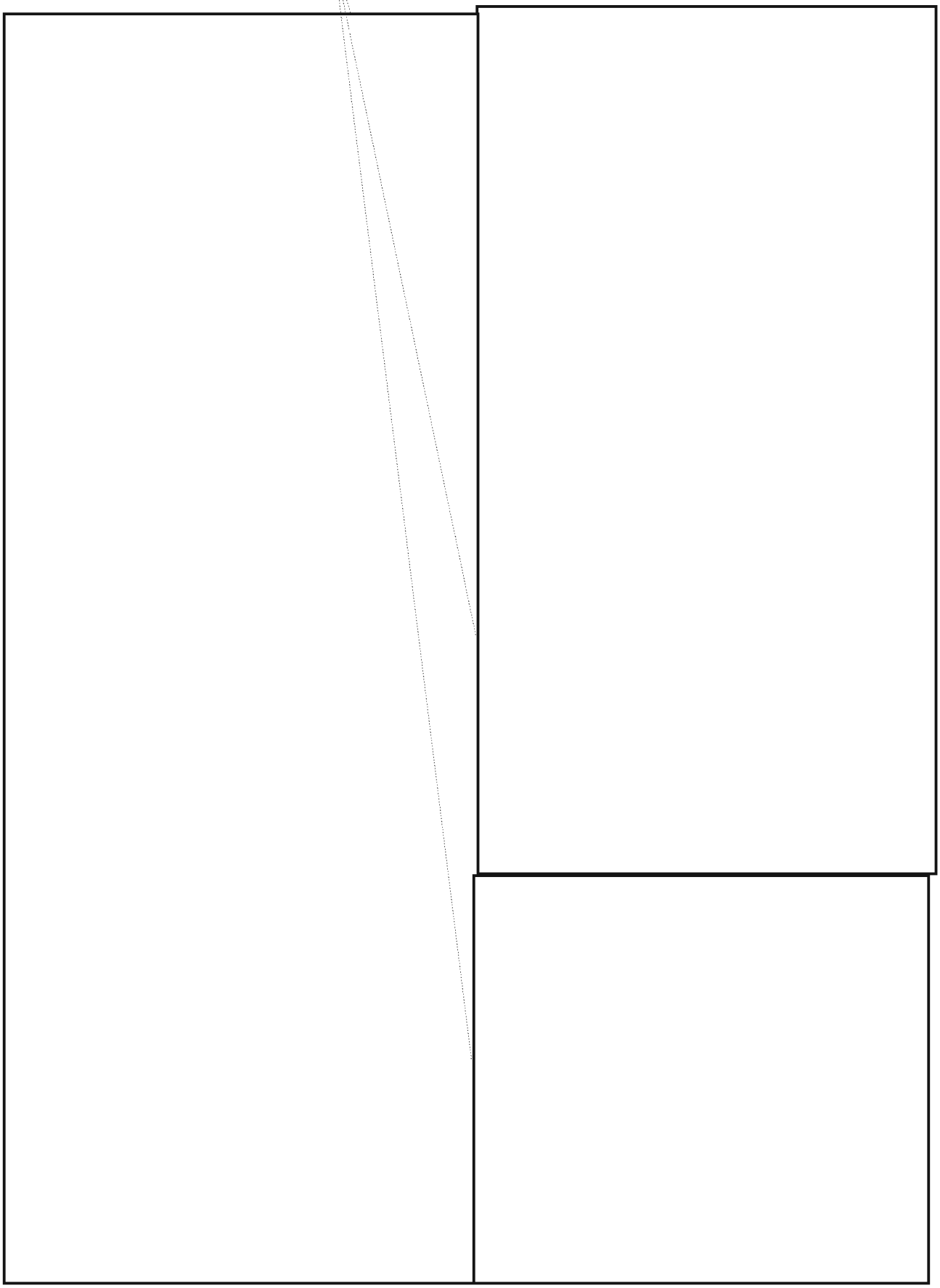
The Challenge: (U)

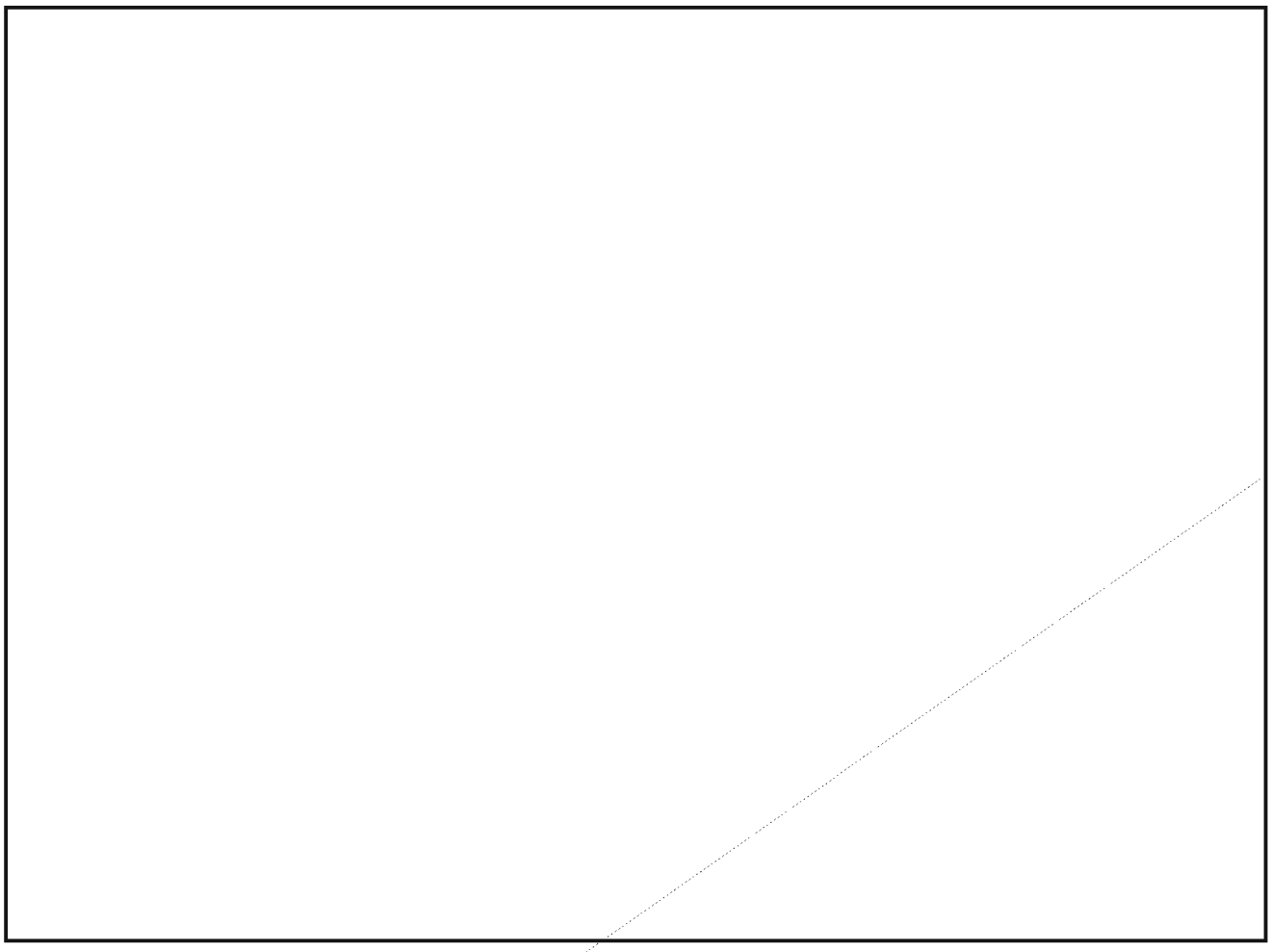
~~(S-CCO)~~ The fledging effort in Production (PROD) faced a number of technical challenges in the fifties: a growing number of technology changes on the part of the targets, [redacted]

I became a member of this team in October 1949 [but] it was not until early 1957 that we were recognized as Signals Analysts. Until then we were Clerks (General), Engineering Aides (Electronic and/or General), or Communications Analysts/Specialists.

~~(S-CCO)~~ [redacted] this task was levied by the Deputy Director for Operations, Rear Admiral T. R. Kurtz, Jr., USN.

[redacted]



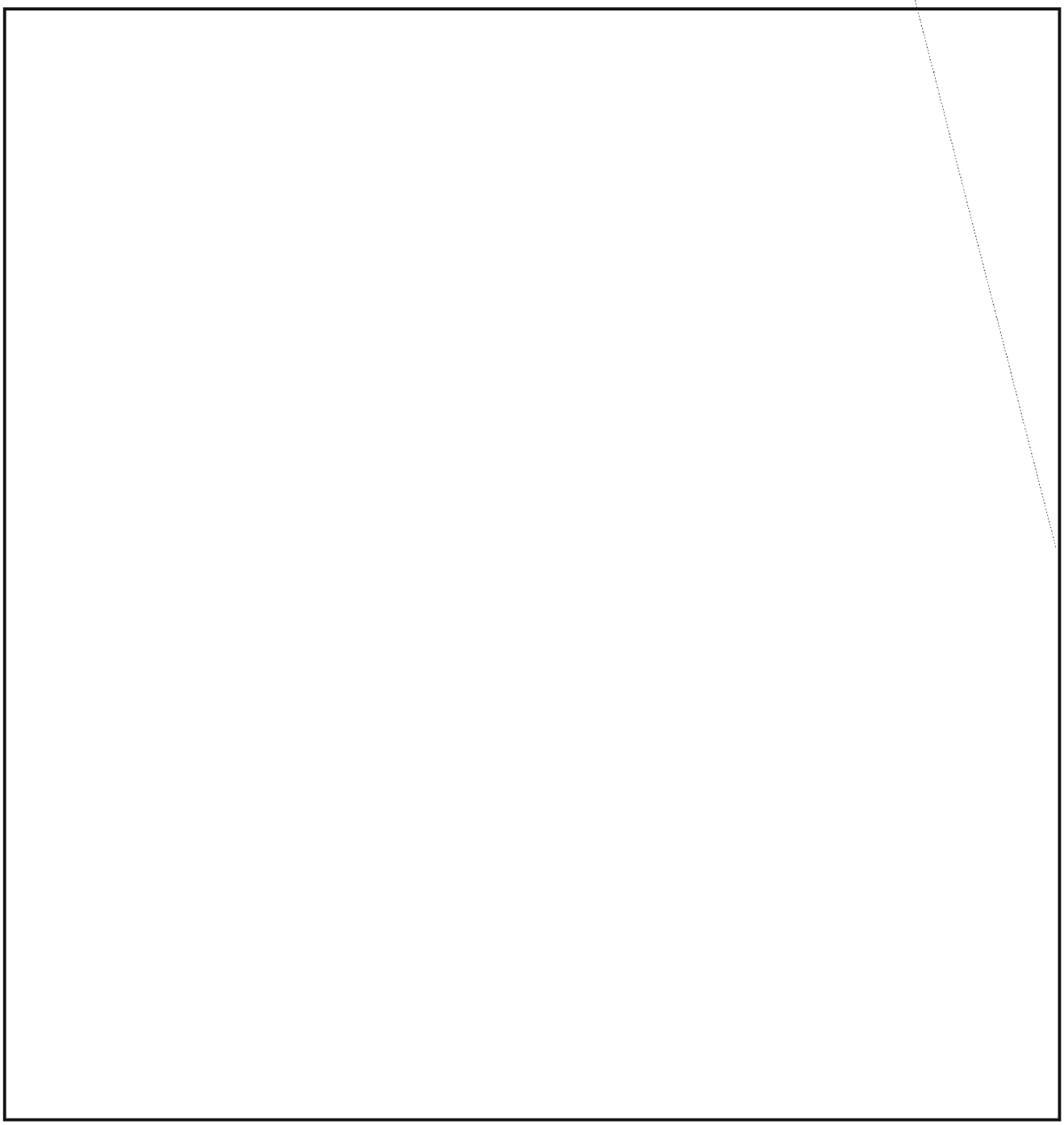


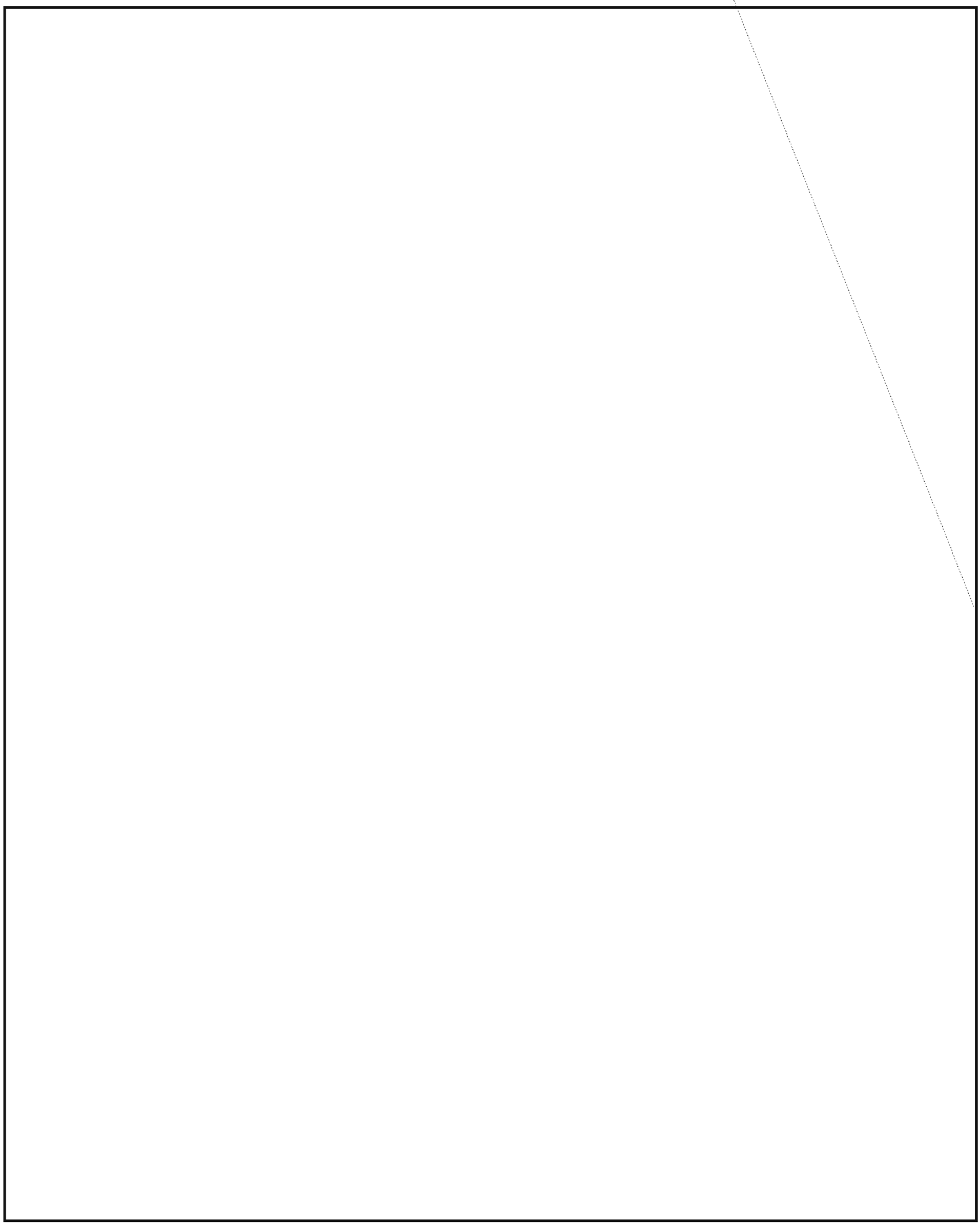
EO 1.4.(c)
P.L. 86-36

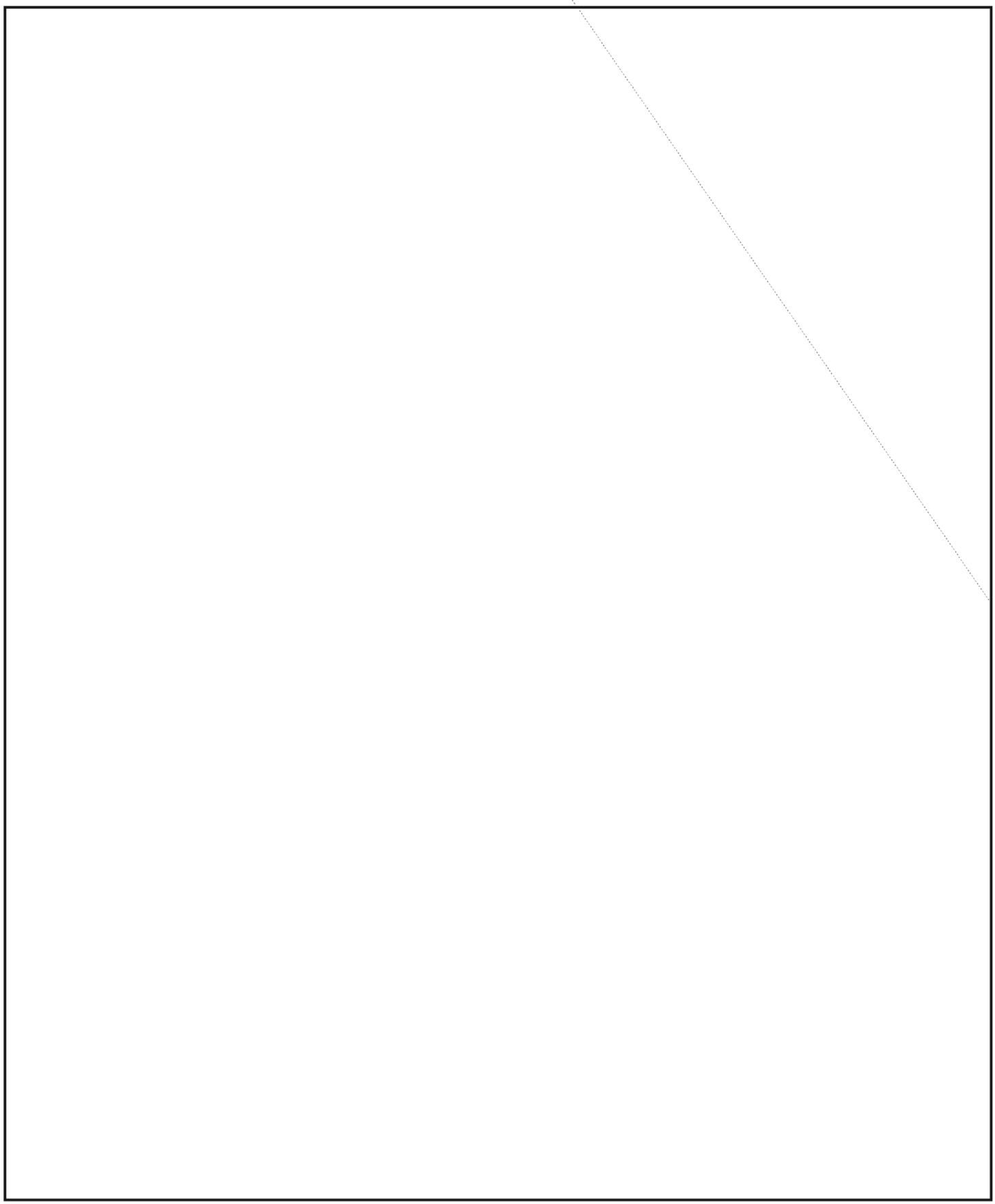
An Example of Intelligence Community Synergy

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

P.L. 86-36

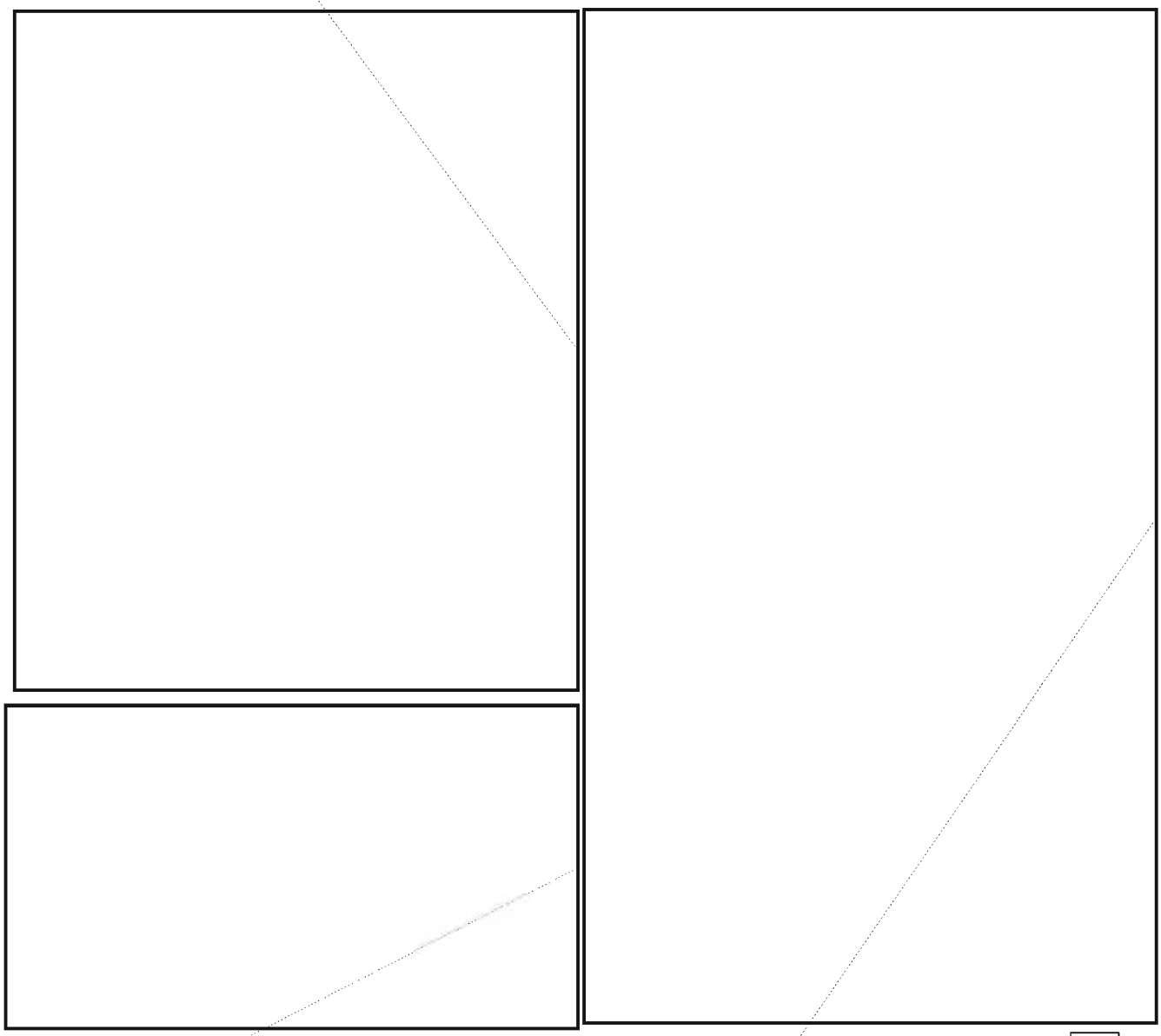






~~TOP SECRET~~

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



Κλ

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

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

SENTINEL: A Look at Database Security ~~(FOUO)~~

by [redacted]

P.L. 86-36

(U) The need to store data classified at many different levels in one database prompted the creation of the SENTINEL database security filter. Managers, analysts and collectors at NSA need to make decisions based on data from many different sources and classification levels. With shrinking budgets and personnel cuts, individuals are expected to manage more information and make broader decisions than in the past.

Approaches to security (U)

(U) The most secure solution to the database security issue is to start at the ground level. Acquire a secure operating system, such as Trusted Solaris, as the foundation. Next place a secure relational database management system on top of this to form a completely secure system. Unfortunately, this solution is more expensive, harder to use, and more difficult to administer than a traditional operating system and database management system. In addition to cost and usability, this solution requires you to supply all the users of your system with the same configuration, which incurs further cost.

(U) Another solution, and the one taken by SENTINEL, is to take a traditional operating system such as SunOS, Solaris, or AIX and use a traditional database management system such as SYBASE. This solution is not as secure as the one mentioned above but fits into the existing computer architecture, which does not include trusted operating systems and database management systems. SENTINEL was created to prevent accidental data disclosure but not a malicious attack.

What is SENTINEL? (U)

(U) SENTINEL is a security filter for SYBASE databases which provides multi-level security down to the row level. SYBASE alone provides security at the table level, but this is not good enough for SENTINEL's users, who demand finer granularity down to the row level. For those not familiar with relational database management systems, the composition of today's relational database management systems consist of application databases at the top. Databases are composed of tables and tables are composed of rows. SENTINEL insures a user will only see the rows of data for which he/she is cleared to access.

(U) The SENTINEL security filter is an integral part of project PLUS. PLUS has 1600 users worldwide located at the CSGs, RSOCs, field sites, other Key Components and DO. PLUS gives users feedback about SIGINT production as a whole and where they fit into the SIGINT production system. SENTINEL is used in [redacted] and a Second Party project called [redacted].

(U) SENTINEL has been certified by J06 at the C2 level for in-house use. The C2 criteria can be found in the Orange Book. For the full criteria, go to **http://nectarine.q.nsa/REGS/rainbow/**

orange on the NSA network. For those not familiar with the Orange Book criteria, D is the lowest or least secure level and A is the highest or most secure level with C and B in between.

How it works (U)

(U) SENTINEL is a SYBASE Open Server application program that runs between the user application, or client, and the backend SYBASE server program. It acts like a watchdog in front of the user's application database preventing unauthorized access to data. SENTINEL intercepts each Structured Query Language (SQL) request sent to the SYBASE server, modifies the request by adding the appropriate security information and forwards the modified request to the SYBASE server for processing. Once SYBASE receives this modified SQL request, it processes the request and sends the results back through SENTINEL, in pass through mode, to the user process. Pass through mode means the data is unaltered.

(U) The SENTINEL database is used to store all the pertinent security information about users, what databases they have access to and the clearance level of the databases. Storing the user classification in a separate location from the data classification is a characteristic of secure systems. Again, consult the Orange Book for more information. The SENTINEL database can be updated manually or automatically. An example of the automatic mode can be found in Project PLUS which has written a program to query the SPECLR clearance database nightly and transfer that information to the SENTINEL database. In this mode, SENTINEL will have current security information about its users. It will know, for instance, if a user has lost the TK clearance from one day to the next.

(U) SENTINEL will have current security information about its users. It will know, for instance, if a user has lost the TK clearance from one day to the next

(U) SENTINEL expects a security label to be attached to every row in a database and to every database user. This label contains three components: a hierarchical component for storing clearance information such as Top Secret, Confidential, etc.; a privacy component which restricts releasability privileges; and a compartment component which stores need to know items such as TK, VRK, BYEMAN, etc. The clearance component can store 16 different combinations of mnemonics. The privacy component supports a maximum of 32 privacy labels. The compartment component supports a maximum of 1024 compartments. These components are stored as bit mapped fields where each bit or pattern of bits corresponds to a mnemonic such as TK, VRK, SECRET etc. The decision to store this information as bits was developed in the interest of space and speed. Since a bit, which can either be a 1 or a 0, is the smallest unit in a computer, it does not take up much space. Manipulation of bits in a computer is also very fast.

(U) At the heart of SENTINEL is the SQL parser. It breaks SQL statements down into separate components which are then passed to the processing module of SENTINEL. This processing module inserts limiting information, derived from the SENTINEL database, about the user into the user's SQL and then forwards the modified SQL on to the SYBASE server for processing. For instance, a user query might say something like, "I want to see all rows in the employee table." SENTINEL modifies that query to say "I want to see all rows in the employee table that are at my clearance level," or, more specifically, "I want to see all rows in the employee table that are Top Secret or below, TK and VRK." The information used to modify the query comes from the SENTINEL database.

(U) In addition to the row level security provided by SENTINEL, other security features are in place. The first restriction SENTINEL imposes is no user accounts on the backend SYBASE server. We don't want an ordinary user to bypass SENTINEL by logging on to the backend database to access information. Users log in to SENTINEL using their unsecured Agency SID and password. SENTINEL uses this account to retrieve the sid and password of the user's secured account. Using this information, a secured connection is established, the unsecured connection is terminated and

the password to the secured account is changed. This level of security differentiates between a user's access to a database in secured mode versus access to a database in an unsecured mode. Access to secured databases is granted to a user through the secured sid. Attempts to use a secured database under an unsecured SID will be prevented by the SYBASE server's database level access control mechanism.

(U) One of the main reasons SENTINEL only works with the SYBASE relational database management system is that it is the only widespread database management system at the Agency that supports bit manipulation. There are other products on the market that perform database security such as ORACLE's Row Level Security product, but this requires developers to purchase ORACLE whereas SYBASE is essentially "free" since NSA has a site license for SYBASE.

SENTINEL Operation (U)

(U) SENTINEL runs in the background, which means there is nothing to see. It has no user interface, so you will never see a SENTINEL icon on your computer screen. SENTINEL operates in two modes. In the first mode, developers can include SENTINEL library "C" language modules in their "C" programs to create their own custom applications that are secure. This is what project PLUS has done. The last method to access SENTINEL is through the use of stored procedures. Stored procedures are collections of SQL statements used to perform a task or set of tasks designated by the user. These stored procedure calls can be sent to SENTINEL through a "C" language program or an ISQL session. An ISQL session allows its user to type and send SQL without having to know a programming language such as "C". This last mode provides the greatest flexibility because it allows a user to send any allowable SQL and receive results instantly while still being assured they will receive only the data for which they are cleared. In addition to the standard SYBASE stored procedures, the SENTINEL developers have added many security specific stored procedures. These stored procedures allow the user to set and retrieve their clearance, privacy and compartment levels within allowable bounds. A user is allowed to downgrade their clearance level to give a demo, for instance, but is never allowed to raise their clearance level beyond that which is set by the SENTINEL administrator.

Conclusion (U)

P.L. 86-36

(U) The long-range goal of database security is to have a product that can access many different types of databases, not just SYBASE. This product would not greatly hinder the performance of database retrievals and updates. It would also require minimal updates to the user's application to take advantage of the security aspects. Until such an application is found, SENTINEL is here to fulfil the database security requirement.

~~(FOUO)~~ Mr. [redacted] started his Agency career twelve years ago as a computer analyst in the R directorate. Since then, he has worked in a variety of areas from contracting officer's representative (COR) to software development and system support. He currently works in E223 as the SENTINEL project leader. When the weather is nice, Mr. [redacted] can be found riding his bicycle. He would like to thank [redacted] and [redacted] for their enhancements to this article.

Kλ

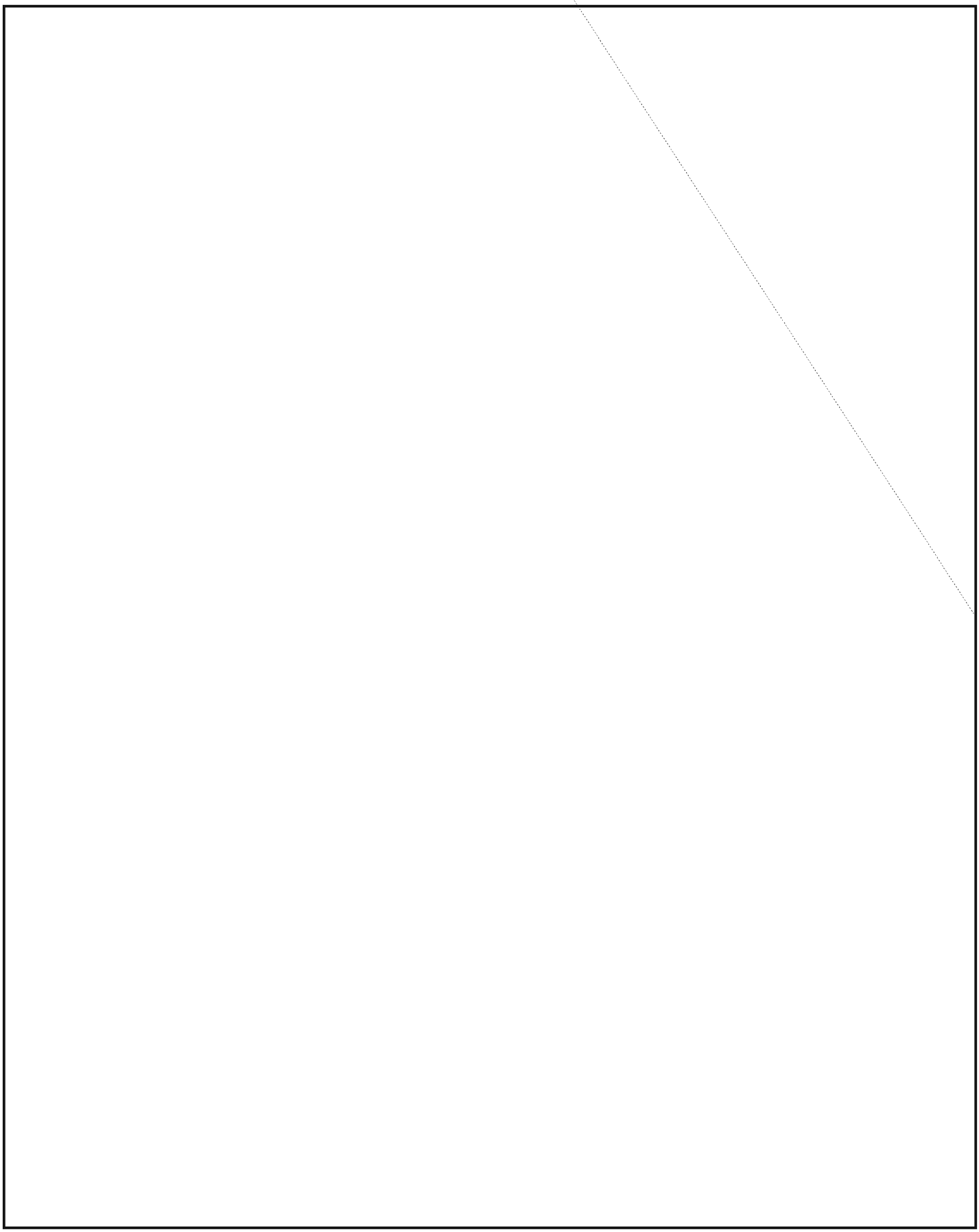
~~TOP SECRET UMBRA~~

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

by [redacted] P.L. 86-36

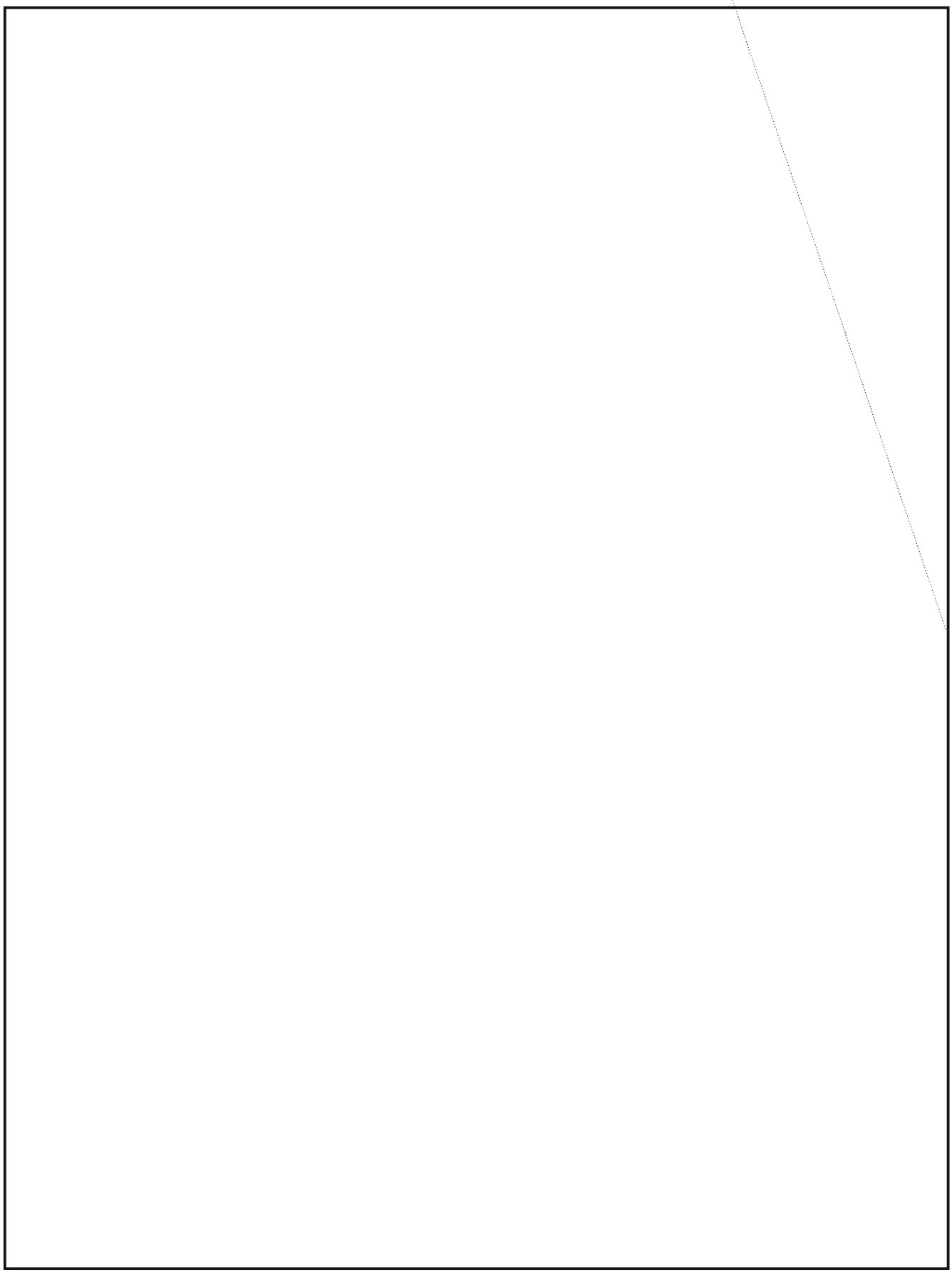
[redacted]

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

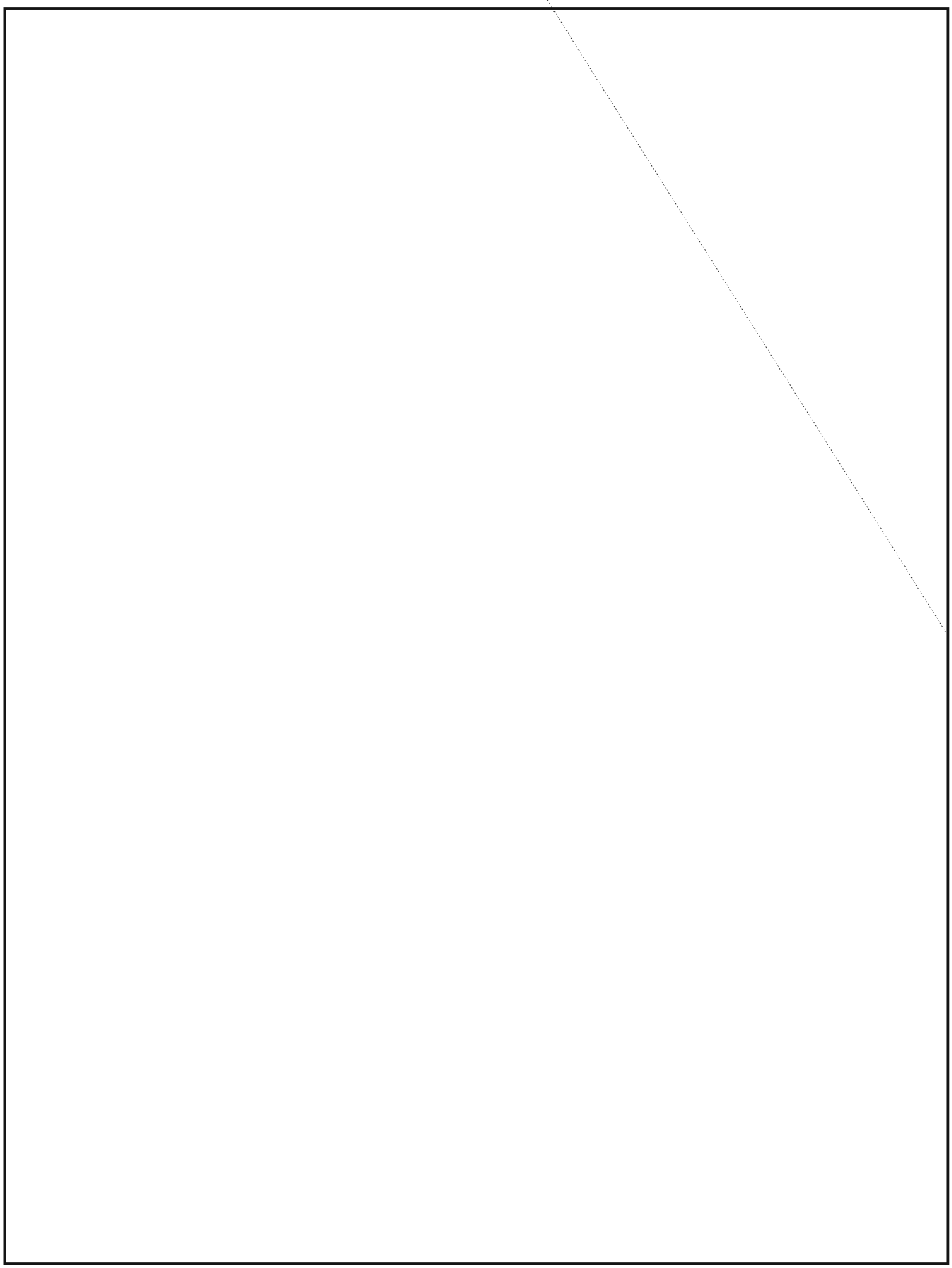


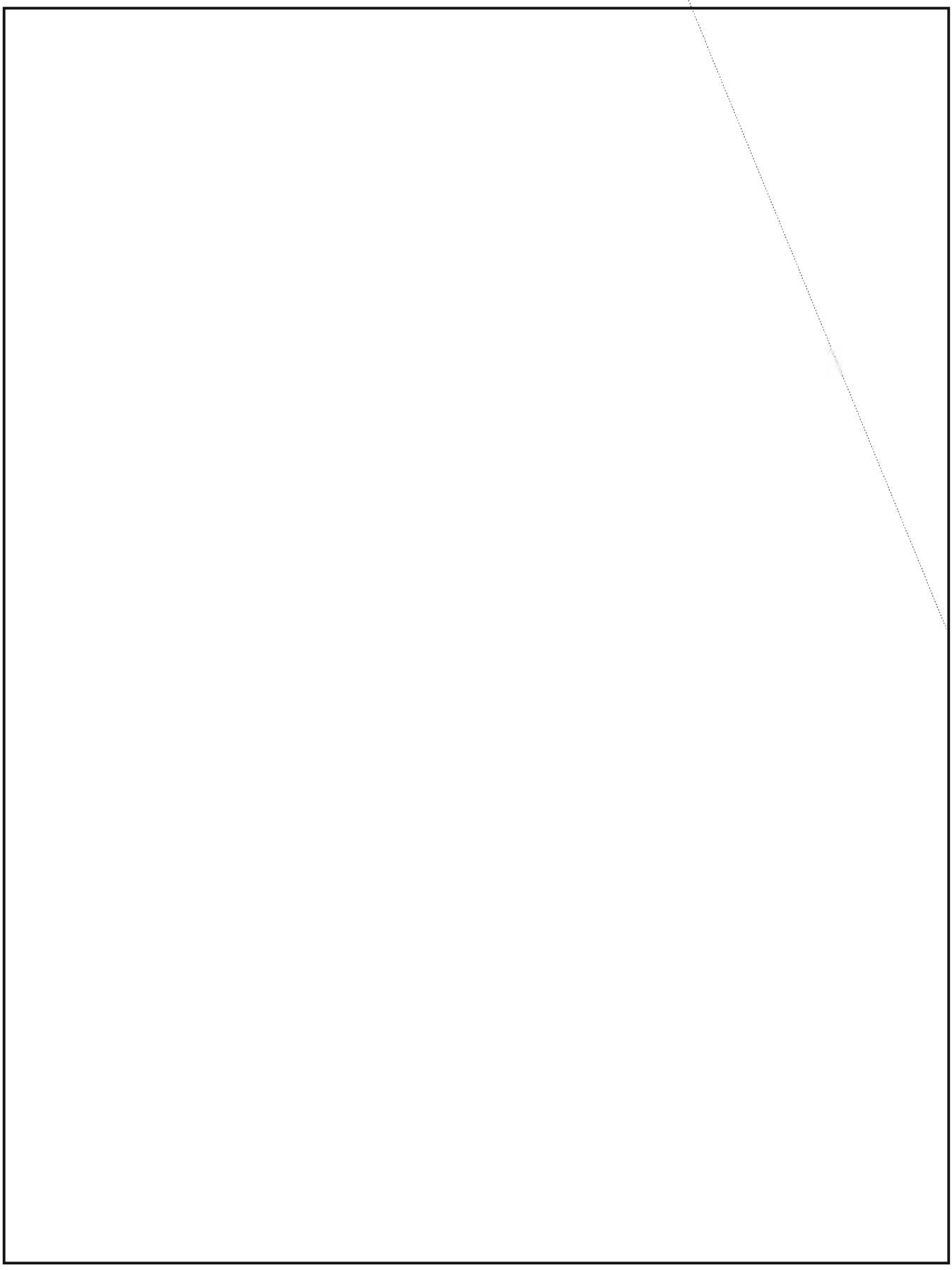
~~TOP SECRET UMBRA~~

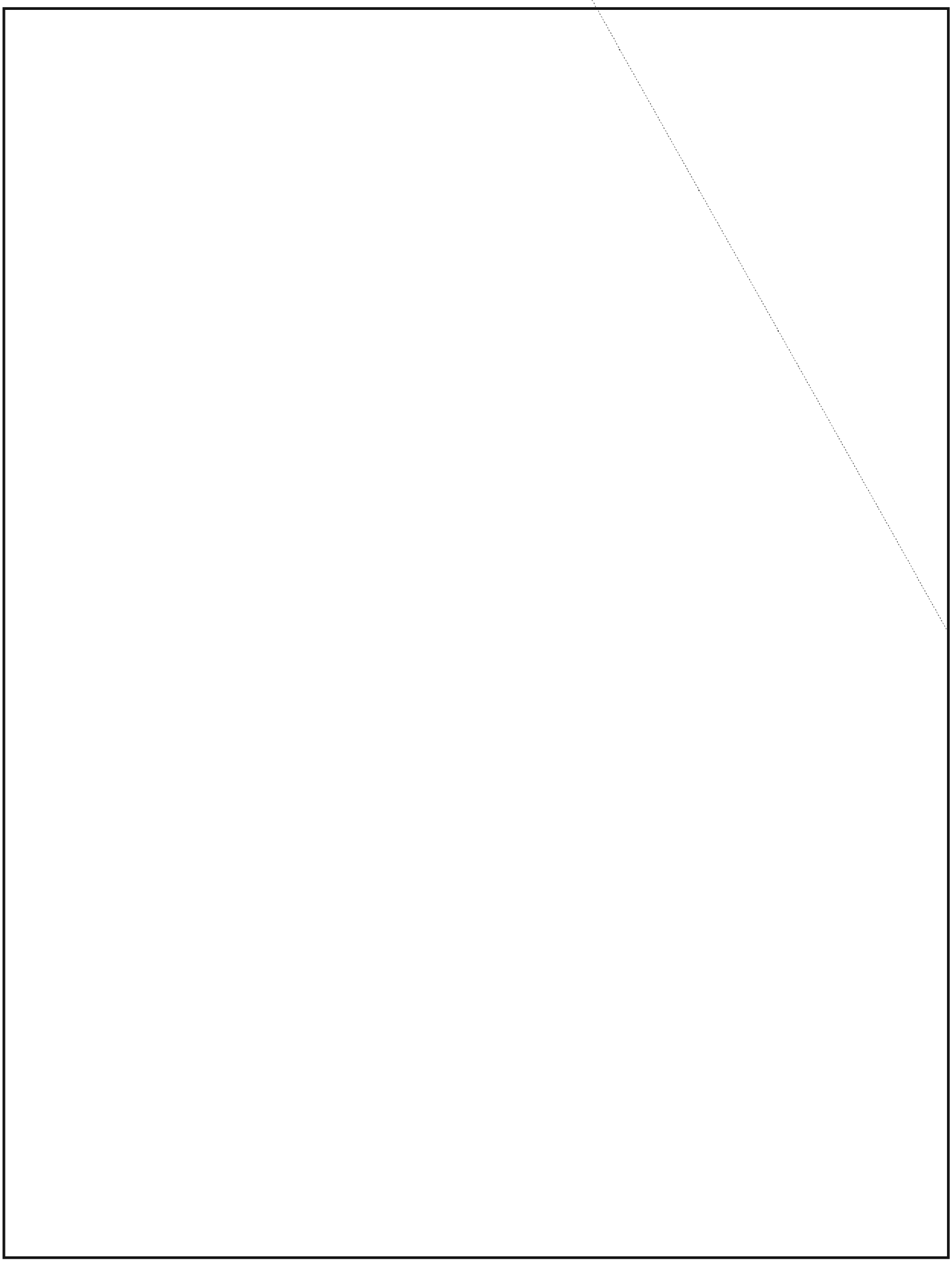
EO 1.4.(c)
P.L. 86-36

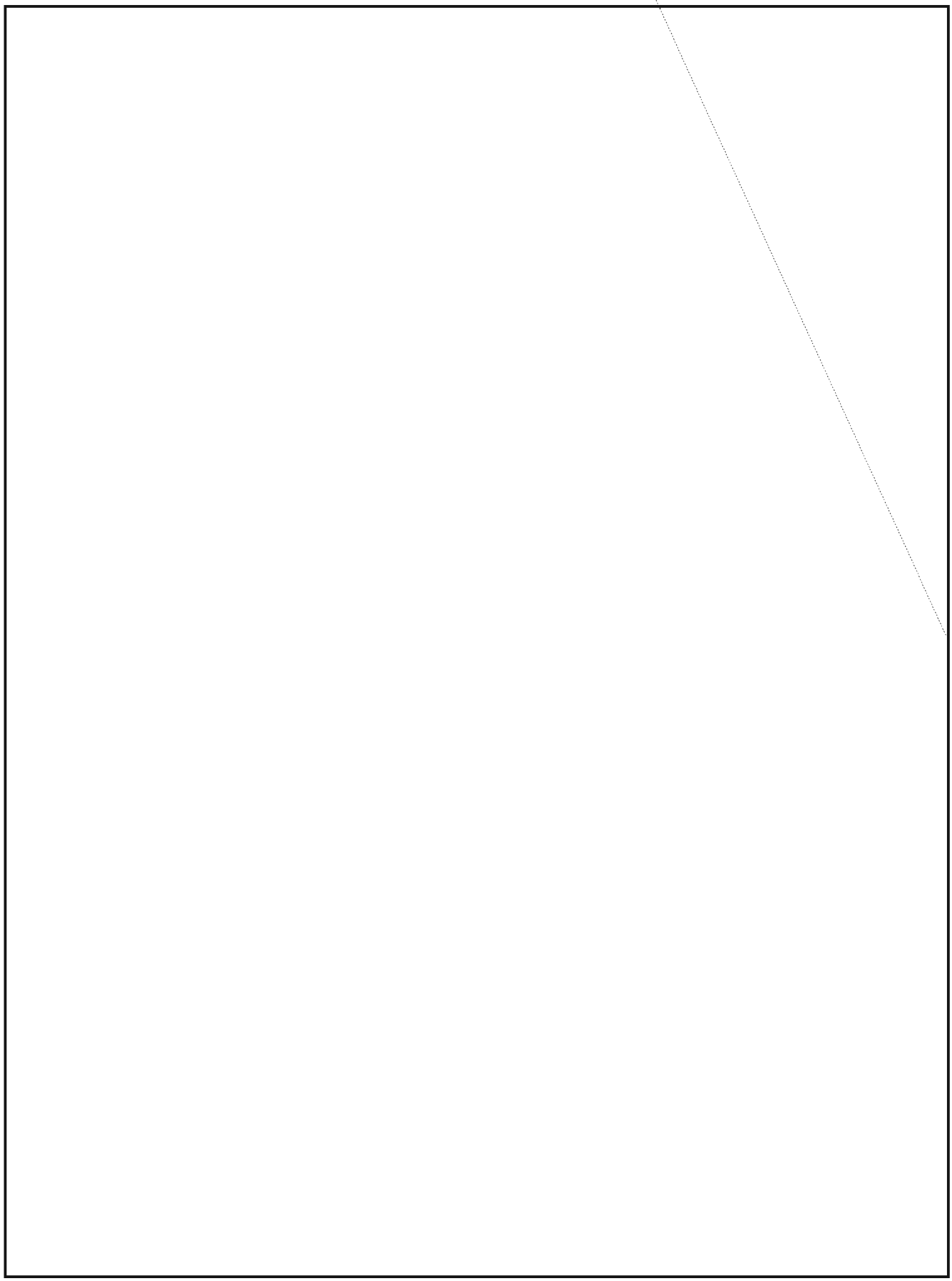


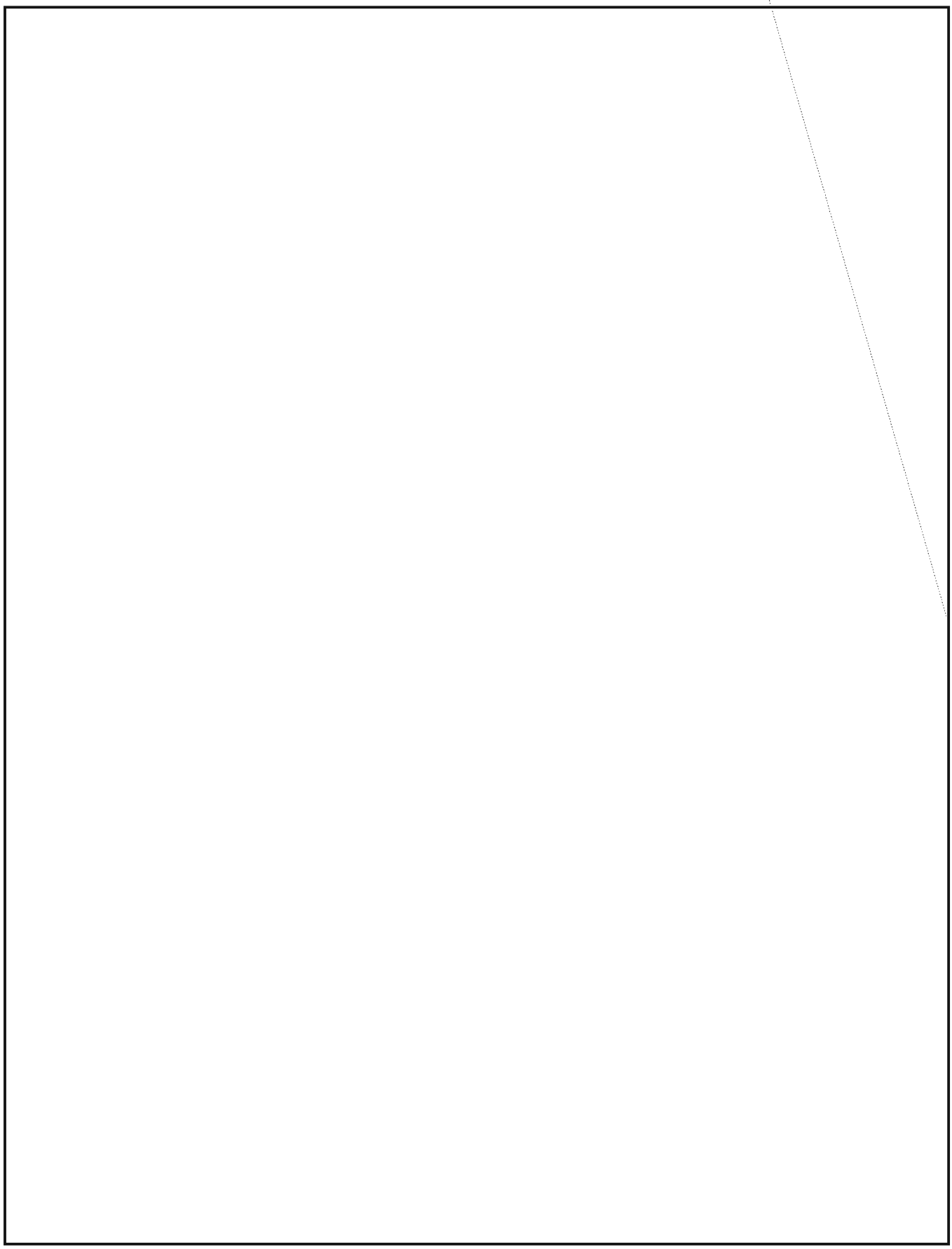
EO 1.4.(c)
P.L. 86-36

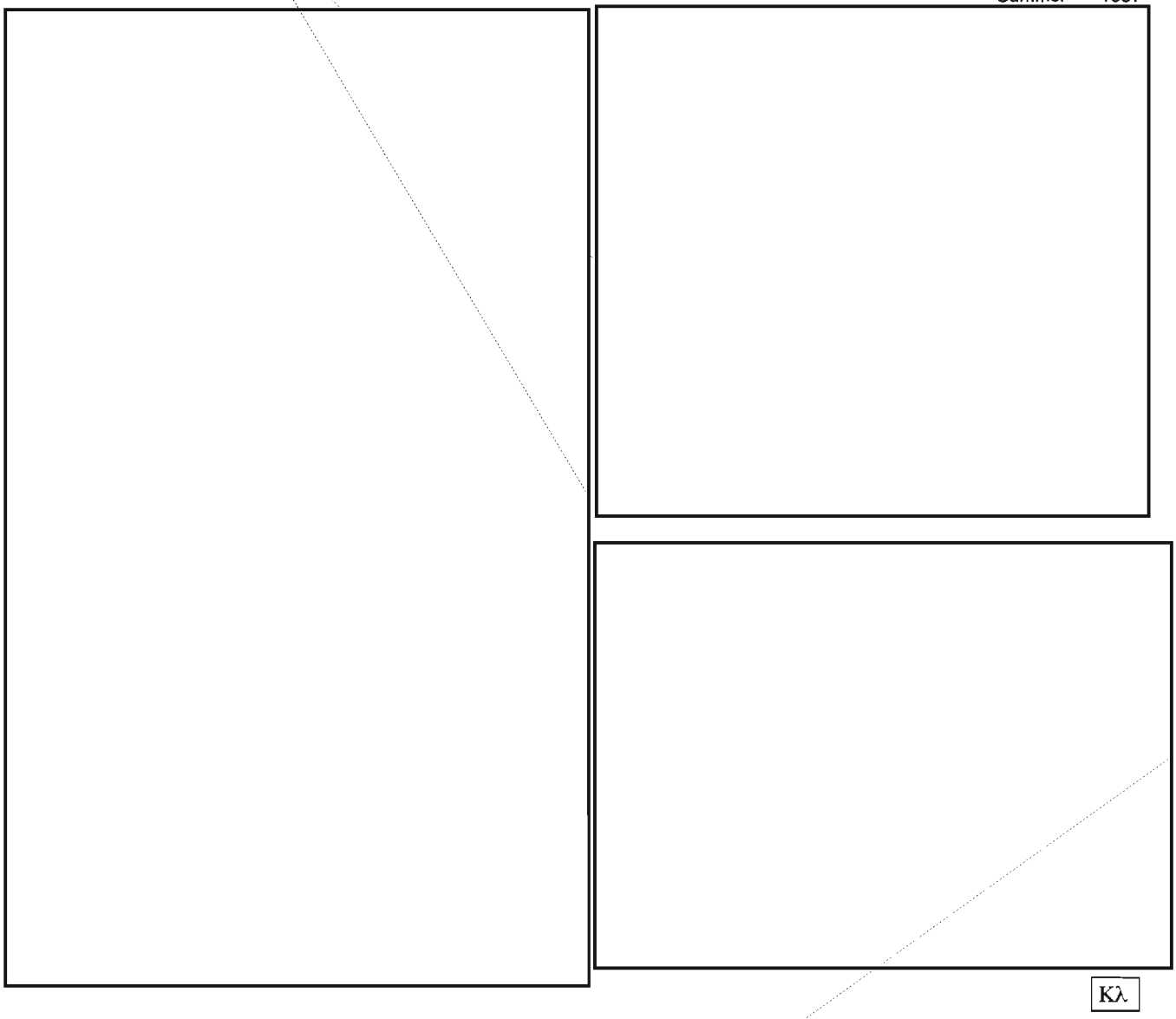






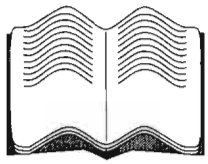






Kλ

Book Review (U)



Steve McConnell. Rapid Development
Redmond: Microsoft Press, 1996. 647 pp.

Reviewed by [redacted] P.L. 86-36

(U) Steve McConnell is chief software engineer at Construx Software Builders, Inc., a Seattle-based software development corporation. He is the author of *Code Complete*, as well as the editor of IEEE Software's "Best Practices" column.

(U) *Rapid Development* is a very well-organized, easy-to-follow book. Icons, specifying such things as best practices, hard data, classic mistakes, further reading and cross-references are placed in the margins. The bibliography is impressive: over 200 references to classic software articles and books, such as Yourdon's *Modern Structured Analysis*, Booch's *Object-Oriented Analysis and Design: With Applications*, even Tom Peters' *Thriving on Chaos: Handbook for a Management Revolution*. Each chapter concludes with a further reading section, which reflects the resources McConnell used for that particular chapter. He uses case studies involving a mythical software development organization, Giga-Safe, which builds business-oriented tools. These case studies show the right and wrong way to manage a program, using very close-to-life examples. As with Scott Adams of *Dilbert* fame, you get a feeling that Mr. McConnell has worked as a software developer for the National Security Agency.

(U) Do you as a software developer want to try to avoid such things as "feature creep" (a.k.a. "requirements creep)", code-like-hell programming, insufficient or inadequate planning, omission of tasks, or unrealistic expectations? Then this is the book you should take time out from your hectic schedule to read.

(U) The subtitle of *Rapid Development* is *Taming Wild Software Schedules*. In Part I of this three-part book, "Efficient Development," Mr. McConnell does a tremendous job of laying out the pitfalls of what he terms the "slow-development" problem and from there shows the path to Rapid Development. He states very succinctly that the slow-development problem pervades the software industry and describes it in a Summary of 36 Classic Software Mistakes, under four sub-headings: People-Related, Process-Related, Product-Related, and Technology-Related Mistakes. In other words, the classic problems that affect your wild software schedule. Additionally, the first part covers the following topics, with a chapter devoted to each: Rapid-Development Strategy; Classic Mistakes; Software Development Fundamentals; and Risk Management.

(U) Part II, "Rapid Development," covers what should be done by Program Managers and Team Leaders to migrate from slow to rapid development by showing the reader how to plan a project from start to finish, how to avoid the classic mistakes, how to build a team, choosing a life-cycle (Spiral, Evolutionary, Staged Delivery, etc.), and how to mitigate risk. He uses pictures, graphs, cartoons, diagrams, statistics, flow charts, and even a dinner menu to illustrate his points. This section covers Core Issues in Rapid Development; Lifecycle Planning; Estimation; Scheduling; Customer-Oriented Development; Motivation; Teamwork; Team Structure; Feature Set Control; Productivity Tools; and Project Recovery. The two chapters devoted to teamwork and team structure are especially informative.

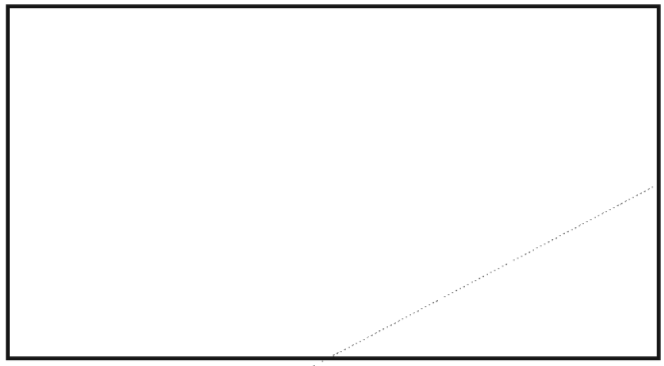
(U) Part III, "Best Practices," finishes the book with a summation of 27 simple yet effective tools to build a quality software product. These practices include: Change Board; Daily Build and Smoke Test; Designing for Change; Evolutionary Delivery; Evolutionary Prototyping; Goal Setting; Inspections; Joint Application Development (JAD); Lifecycle Model Selection; Measurement; Miniature Milestones; Outsourcing; Principled Negotiation; Productivity Environments; Rapid-Development Languages; Requirements Scrubbing; Reuse; Signing Up; Spiral Lifecycle Model; Staged Delivery; Theory-W Management; Throwaway Prototyping; Timebox Development; Tools Group; and Top-10 Risks list.

(U) It's been said that the beginning of a solution is realizing just what the problem is. *Rapid Development* shows how to solve problems incrementally. It is a step-by-step reference on how to go from slow development to rapid development; this will show the path to better software engineering and how to deliver a quality product on time and within budget to a satisfied customer.

(U) You would think that a book about software development strategy would be rather dry reading, but Mr. McConnell adds a bit of humor to the text by comparing things like Classic Software Mistakes to watching reruns of *Gilligan's Island*.

(U) The main target audience for this book is the Technical Leaders of software development efforts, however, the book should also be used by supervisors and managers of Technical organizations to understand what their Team Leaders are talking about. The goal of the work is well-stated in the Preface: "[to] lay out in pragmatic terms why many of our most common views about rapid development are fundamentally broken...and to advocate its own small revolution in software-development practices." And that goal has not only been met, but met very well.

(U) I highly recommend this book as the next much-highlighted, marked-in-the-margins, dog-eared, no-you-cannot-borrow-it-get-one-of-your-own books for every software developer, team leader and technical manager.



Kλ

P.L. 86-36

Editorial Policy:

(U) Technical articles are preferred over those relating to management, shorter over longer (under 3,500 words). Emphasis should be on improving NSA's technical performance; articles should be aimed at explaining developments in one's career field to those outside it. Readers are invited to contribute conference reports and reviews of books, articles, software, and hardware that relate to our missions or to any of our disciplines. Editorials are also welcome, as is humor. Submissions may be published anonymously, but the identity of the author must be known to the editor.

Submitting Articles:

(N.B. If the following instructions are a mystery to you and your local ADP support is no help, please feel free to contact the CRYPTOLOG editor on 963-5283s or cryplog@p.nsa.)

~~(FOUO)~~ Send a soft copy via e-mail to **cryplog@nsa**, or send a hard copy accompanied by a labelled diskette to the editor at P02 in 2C099, Ops. 1.

Guidance:

For maximum efficiency (as far as possible within the limits of your word processor):

- Classify all paragraphs.
- Do not type your article in capital letters.
- Label all diskettes, identifying hardware (operating system: DOS, UNIX), density and type of word processor used, filenames, your name, organization, building, and phone number.
- FrameMaker format is preferred; ASCII text is also fine. *(FrameMaker users: while we welcome graphics, please include them in the file as separate objects rather than in Anchored Frames as these frames are nearly impossible to reformat to our standard.)* The editor will be happy to e-mail a CRYPTOLOG template on request. Another option is to use J33's document conversion service (CLEANEX); instructions for e-mailing files for coversion can be found at **http://www.j33.j.nsa/q6/q623/cleanex/clean.html**.