Description of document:	National Security Agency (NSA) Oral History of [NAME REDACTED] Senior Technical Leader for the Custom Solutions Group of the Information Assurance Directorate (IAD), 2008
Requested date:	25-June-2022
Release date:	25-May-2023
Posted date:	26-June-2023
Source of document:	FOIA Request National Security Agency Attn: FOIA/PA Office 9800 Savage Road, Suite 6932 Fort George G. Meade, MD 20755-6932 Fax: 443-479-3612 Online Request Form

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND 20755-6000

Serial: MDR-114597
25 May 2023

This responds to your request of 25 June 2022 to have the transcript of the oral history NSA OH 2008-81 reviewed for declassification. The material has been reviewed under the Mandatory Declassification Review (MDR) requirements of Executive Order (E.O.) 13526 and is enclosed. We have determined that some of the information in the material requires protection.

Section 3.5 (c) of E.O. 13526, allows for the protection afforded to information under the provisions of law. Therefore, the names of NSA/CSS employees and information that would reveal NSA/CSS functions and activities have been protected in accordance with Section 6, Public Law 86-36 (50 U.S. Code 3605, formerly 50 U.S. Code 402 note).

Please be advised that the responsive document includes other government agencies' information. Because we are unable to make a determination as to the releasability of other agencies' information, the subject document was referred to the appropriate agencies for review. At the time of this letter, the responses are outstanding. However, we were able to isolate the other agencies' equities, so we have protected them using the other government agency (OGA) redaction code.

Since your request for declassification has been denied you are hereby advised of this Agency's appeal procedures. Any person denied access to information may file an appeal to the NSA/CSS MDR Appeal Authority. **The appeal must be postmarked no later than 60 calendar days after the date of the denial letter.** The appeal shall be in writing addressed to the NSA/CSS MDR Appeal Authority (P133), National Security Agency, 9800 Savage Road, STE 6881, Fort George G. Meade, MD 20755-6881. The appeal shall reference the initial denial of access and shall contain, in sufficient detail and

particularity, the grounds upon which the requester believes the release of information is required. The NSA/CSS MDR Appeal Authority will endeavor to respond to the appeal within 60 working days after receipt of the appeal.

Sincerely,

Jacqueline M. Amacher

Jacqueline M. Amacher
Chief
Declassification Services

Encl:
a/s

OHNR: OH-2008-81 **DOI:** 23 December 2008
TRSID: [redacted] **DTR:** 12 January 2009
QCSID: [redacted] **Text Review:** 21 Jan 09
INAME: [redacted] **Text w/Tape:**
IPLACE: NSA, SAB 2 Building, Oral History Room, Ft. Meade, MD
IVIEWER: COOLEY, David P. (Dave)

Cooley: This is NSA Oral History 2008-81. Today is 23 December 2008, and we are talking to [redacted] Senior Technical Leader for the Custom Solutions Group of the Information Assurance Directorate. [redacted] will be retiring at the end of the month and has consented to provide us a career retrospective interview. I am David Cooley, the Oral Historian for the Center for Cryptologic History. This interview is being recorded in the SAB 2 Oral History Room. The classification of this interview is ~~TOP SECRET//COMINT~~. We can adjust this classification at the end if need be [redacted] the Center for Cryptologic History wants to thank you for taking time out of you busy schedule to participate in this career retrospective oral history interview. As this is a career retrospective, would you provide us an overview of your academic background and how you came to work at NSA, and your early career at NSA?

[redacted] Back when I was in college, I wanted to become an electronics engineer. At the end of my junior year, the Agency was there interviewing people. I thought it'd be a great opportunity to get some real experience working with electronics. I came down here for summer hire; worked in the production shop in the satellite group. I found the work very interesting, very challenging. I went back, received my degree, and decided to come and work here at the Agency full time. Also an incentive at that time is that [redacted] Upon completion of my schooling, I stayed with the Agency. And I have found my careers here wonderful. They have been challenging. If you get tired of this little area or a certain area, there's always another area you can move into. I started off with equipment design. I was able to move into management. I ended up having some interesting discussions with the logistics people, the production people here; we got into reliability issues. I first worked in the satellite world where we're very much interested in reliability of the components. Matter of fact, that was the most important thing--is the quality of the parts going up there. After that, then, we had some interesting reliability discussions as to whether a part was adequate or not adequate. It became very challenging to sit down and look at some of the failures of the equipment, saying, "Gee, can...? Is

Derived From: NSA/CSSM 1-52
Dated: 8 January 2007
Declassify On: 20320108

this equipment still good enough to launch for a satellite? Have I got some reservations about it?" If we're talking here about a twenty-thousand-dollar piece of equipment, forty-thousand dollars, but the satellite is running into the millions of dollars. So it's not the cost of the crypto equipment that was at stake here, it was really the cost of the satellite. And if we ever lost a satellite, the other ramification is: how long would it take us to find a replacement satellite to go in orbit to fill in that hole in our -- either our communications networks or in our intelligence networks. After working in the space community for about ten years in the research and development area, I stayed in IAD, went over to the production side, ran some production contracts. At which point, then, I migrated into the tactical radio (B% in) about the mid-'90s. I moved into tactical radios and to systems engineering. And my last couple of years here in the Agency has been with the crypto-modernization effort. It has been an interesting challenge to sit down with the various services, look at their systems, and try and explain to them where there are ways they could enhance the security with relatively no impact to their system. Most of the services, when they come in, are interested in just, "I want a replacement for the boxes that are out there. I don't want any enhancements; don't want any changes." But when you sit down and explain to them the additional benefits we could have--such as when you talk to software downloads (B% and) equipment, everything's become programmable. And you ask them, "Are you concerned about anybody altering your software?" And the answer would usually come back, "Yes, we are," but they weren't sure how to do it. So we'd sit down and discuss with them the cryptographic techniques that could be applied to make that software really only changed by authorized people. And then, the other area was, "Well, we make a lot of changes. Do we have to always go back to NSA?" And the answer was, "No, you don't have to. There are good commercial software packages--algorithms--out there you could use. The main thing is that you take the time to actually protect your software accordingly." It's been a great career. We have wonderful people here that are very challenging

Cooley: Where did you go to do your undergraduate work?

[redacted]

Cooley: [redacted]

Cooley: [redacted]

Cooley: [redacted]

Cooley: Okay, good. Could you describe your work with the Space Shuttle

PL 86-36/50 USC 3605

program and NASA?

[redacted] Certainly. Back in the early '80s, we were doing some work. I was working mainly with the Air Force, trying to protect the Air Force command and control links. At that point the Air Force was going to move from launching their satellites from missiles or rockets, to using the shuttle orbiter. So I was tasked or requested to come up with the concept for the equipments--the architecture--that would protect the command links from the satellite to the shuttle itself. [redacted] The other challenge there is NASA was. felt they were in a [sic] environment that was to be open. They were sharing their knowledge with anybody and everybody 'cause that was part of their charter. We were talking to them one time, and explained to them or. about their command links to the orbiter were subject to being. either denial of service on those communication links or someone could take it over. And they didn't believe us. But for some reason, one of the administrators heard about it and he tasked his people to come up with an analysis of it. [redacted] So again, I was. My task was expanded also to come up with that particular concept. And it's interesting working with the NASA people. They have an entirely different view on things. One of the things. Their primary importance, obviously, is the safety of the crew. And we had some requirements we had to work with that we had never worked before. how do you meet environmental requirements? [redacted]

OGA

PL 86-36/50 USC 3605

OGA

[redacted] So they ended up being some interesting challenges. It was great working with the people, though. Had a great contractor back here that we were... that (B% I) was under contract helping cevelop the equipment. We had a great time.

Cooley: Did ... ? [redacted]

[redacted]

Cooley: [redacted]

[redacted]

Cooley: Okay. Now you had referenced previously your involvement... or about having special assignments with the Challenger...

[redacted] Yes.

Cooley: Problem? Could you talk to us a little bit about that?

[redacted] It wasn't so much I had direct access into it... [redacted] And when Challenger went off unfor... It was ((an)) unfortunate day. I can still remember in the hallway here, we were looking forward to... with excitement for the flight going off. [redacted] And then, it became very depressing when we heard about the Challenger--the accident. Two of the men that worked for me at that time had gone down to NASA. They had trained them on the use of the equipment. They had become very friendly with some of the astronauts. They knew two of the astronauts personally. So it was a tragedy, then, that happened. Then when NASA went through and did the search and rescue--well, not really the rescue--but the search to obtain the classified information and stuff, we had two people going down there--as they brought in the debris from the spacecraft or from the shuttle orbiter--looking for the crypto gear that was on board both the spacecraft and the orbiter itself. Those boxes... There were four boxes on board. They have

PL 86-36/50 USC 3605

been returned here to the Agency. I turned them over to the archives group back in the late '80s. ((The)) boxes were designed to withstand twenty thousand times the force of gravity for shock testing in all axes. When we went to our qualification testing, we hit it twenty-seven times with that shock, never lost a bit. And when they came back, the boxes were in pieces. So it gave you an idea of the tremendous force that occurred when that ex...I'm not so sure it was the explosion that tore the boxes apart as much as when it hit the water.

Cooley: Water, yeah.

[redacted] I mean, the speeds they were traveling when it hit the water, it's like hitting a brick wall. But there were tremendous forces involved in that.

Cooley: What was the most interesting job that you had during your IAD career?

[redacted] That's a tough question to answer. All the jobs were interesting. The work here at the Agency is so varied, it's hard not to find something that's interesting. ((He clears his throat.)) Excuse me. I guess there were two I really enjoyed. Working with NASA because it was something brand new they had not worked with before. We were trying to get with them and explain to them what benefits the security would provide to the orbiter. So it was nice to do that way...a lot of education to the people down there. And they were great people to work with. And then, the last one I really enjoyed is...at the end of my career here, where we're going through modernizing our cryptographic algorithms. Again, it's nice to sit down with people, explain to them the benefits that security can bring. Most of the time, the Agency was considered as a problem or a nuisance or something else--because if the crypto didn't work, they couldn't communicate. If the crypto worked, they loved it. It was good communication links. And more often than not, they were having problems: either the keys were incorrect, they got the wrong key, they didn't have the key. But it didn't matter to them. The fact is the system didn't work because the crypto. So when we got into the crypto-modernization efforts here, trying to talk to them and explain to them what the problems were--why we had to replace the cryptography. Because it's unusual talking to some of the services. They don't mind changing the designs of their equipment to accommodate new technology. But for some reason, the crypto is never supposed to have new technology. And when you sit down and explain to some of them that the cryptography they were using was generated or developed in the '60s, they're shocked. Here it is forty years later; we're still using the same technology from a cryptographic standpoint. So then, they became more understanding what we were trying to do. And again, to sit there and explain to them the benefits we could bring from a security's perspective using some of this stuff with (B% designing) of software, role models so that when you come in. Only people allowed to do certain things can do thing...can do those operations on equipment. For example, we just had a discussion with the Navy. We were saying--about having role models for the equipment--

PL 86-36/50 USC 3605

having it securely done so that not everybody can come up and turn on a box, maintain it, change software, but just certain people. And they were adamant about doing that. They said, "No, we don't want to have any kinds of password protection on the box." And after some discussions, we realize what was bothering them is this was going on a Navy fighter aircraft. They didn't want the pilot to have to sit there and worry about what the password is. If he's in a dog fight and he gets a power glitch and has to reset his crypto, "No, I don't want to worry about it." I said, "You don't have to." And they said, 'Huh?' They were confused. I said, "What you do is, if the person..." As far as I'm concerned in this Agency, if a person cannot get on board a loaded--fully loaded with weapons--an aircraft on a Navy base or on an aircraft carrier, he's got all the authority he needs to turn on the box and operate it. But that doesn't give him the right to change the software. It doesn't give him the right to do the maintenance. So when we design the box, let's just put the password protection for the people who are doing maintenance, for the administrator of the box, people doing software downloads. And when they realized that, they became very eager to do those kinds of things. 'Cause they were p. They were concerned about somebody doing that. But they felt it was all or nothing. So it was an interesting educational experience. And there was [sic] a lot of other services had the same kind of attitude: it was all or nothing. When you sit down and you start talking to them and explaining, "It doesn't have to be 'all or nothing' other than when it comes to the cryptography. For other aspects of the radio which we're not dealing (B% with) security--but it's more availability--it's you call. You make the decisions how you want to handle it." And it's been a challenge, and I think the word's been getting out there slowly. So those have been the two things I've looked forward the most.

Cooley: Did you notice continually in your career here--when you were working with outside customers: one, just a lack of knowledge of what crypto was? And two, if they had some knowledge of it, a lack of ((he pauses)) a lack of the patience to work with it. Do you understand what I ? A lot of issues that you were saying there with the Navy folks...A lot of people don't want to bother with it unless it's .that it's always seamless, right?

[redacted] When I first came here, back in the '60s, there were so many restrictions with the use of the cryptography. It really was hard for the military. They were afraid of violating the directives. And to them, it becomes a criminal offense. If you lose your key, that's a criminal offense. So do you want to go and spend a couple of days in the stockade for this? That was what I think that was the biggest problem. You lose your equipment--it's a criminal offense. It's not just a high-value item; they were criminal offenses for them. So (B% there was) Very reluctant to use it. Then when they were forced to use it, they weren't sure how it worked. So I believe when we started changing things--changing the handling requirements. The first thing, they came up and said, "Well, we'll call it a COMSEC controlled item." It took a lot of the criminal aspects out of it

PL 86-36/50 USC 3605

So now they could say, "Well, you can have the equipment If you lose it, alright, you lost it." No one's going to go to jail no one's going to get shot So I think that did an awful lot to help the services We also opened up In the beginning, when I first came here in the '70s, you had to get a special access for cryptographic information When they opened it up, then we were able to talk to the acquisition people And it was no longer a mystery or a black art They understood a little bit more They still didn't like it because of the rules and restrictions They came later, with a relaxation of that But now, in the last ten to fifteen years, we've had so many military come through here, and they've participated in the programs I believe we have done a great service to the services And when the people come here--that they sit down, they go through it, they get a better understanding of what we're trying to do and appreciation for the fact, "You may not like our crypto equipment because it's burdensome, it's awkward, may cost you something But there's a reason for why we've done it And it does protect your people, your communications And if you really have to go in the clear, that's your call as a commanding officer Because, obviously, the mission's more important then--and the lives of your people--than trying to just keep some of the information protected " So I think the people coming through here have a better appreciation and then been able to go back out into the military And a lot of the partnerships we've had recently with the service acquisition elements has helped a lot--that they're now understanding more what we're trying to accomplish and the rationale behind things They may still not like it There's still some ways to go, but there's a big difference in today s environment than it was when I first came here back in the late '60s

Cooley: Good Mmm hmm What INFOSEC technology do you believe is the greatest contribution ..has made the greatest contribution during your career? What one thing during your career do you think is the real INFOSEC high water mark?

[redacted] Ah ((He pauses)) I think it's happening now, but let me give you a little background And it has to do with the programmability today I think that's the best thing We're making it easier It's become more releasable We can deal with it Technology's moving too fast Back in the '60s, the '70s, the '80s, you built a box, and we were the mainstay We never change When we I did a lot in the space community And they considered the satellite as a truck with boxes bolted onto it for the various technologies Whether it be for the intelligence world or for the communications world, it didn't matter We were always considered part of that truck We were the We were never the payload; we were always the truck We're the vehicle, the bus, that got it from the ground to on orbit and maintained it So they didn't care about the technology changing In 1972, we started what I would consider the first programmable effort At that time, we were trying to do some secure anti-jam systems with both the Air Force and the Navy And anything we had too big, too heavy, too bulky, too slow And they were right We hit every Every requirement we were breaking their

PL 86-36/50 USC 3605

backs on We were exceeding the values they could afford And we actually went out and convinced them to ..or convinced our management through the office level to give them just a small, integrated circuit--that's all, nothing else And we would work with them to put the correct security procedures in We had some good successes (B% E-PLOORS) today has been around since then It's still around today It's the backbone for the Army and the Marines. We have .The Navy's Link-16 system has a (1-2G) there that's out And then we have The Air Force has JTIDS Those programs were done back in '72 It's an imbedded effort But after a couple of years, the...Then the director of communica..deputy director for communications became concerned he was losing control And he took everything back under the NSA's auspices and went back to building black boxes We continued to build black boxes And now, as you know, we are into the embedded effort We're going out with cryptographic modules, software applications. And I think that's the best on the technology We have seen a lot of advances in technology, but the services are looking at it from a perspective of in the '70s, you were only ten percent of my budget In the 2000 time period, if we didn't go with the embedment effort, in the 1990s, without before we started embedding we went to 20 percent or 25 percent So, yes, we were smaller, we were lighter, we were cheaper But we were still more of their budget for the size, the weight, the cost By going to the embedded, we went back down and we're now able to take better advantage of the technology and truly give them a solution which is secure--but it is, in fact, a lot cheaper, more reliable, less power Some of these people have enough stuff (B% at) .Some of our soldiers have enough stuff they're carrying out into the field; they don't need another set of batteries hanging around (B% of) five pounds They don't need an extra radio. They needed something small and integrated And I think that's the best thing we're doing And now that we're going into more of the commercial cryptography where we have the policy that the AES algorithm is strong enough that we can properly implement it with our security requirements and design evaluations, is even making it easier from a [sic] interoperability releaseability standpoint So I think we're going to find some very big benefits in what's going on in about the last five years and what'll go on for about the next five to eight years

Cooley: Okay, good What do you believe is the greatest challenge in the future for the Information Assurance Directorate?

[redacted] In reflecting on the biggest challenge that's facing IAD today, I believe there are three kinds of customers out there We kind of use the terms loosely, and it gets confusing I have a customer--which is [sic] the acquisition elements for the services They're required to come up with new equipment designs and to do the actual procurement for the services We have another customer set up there called the operators the people in the field who have to live with the boxes, they have to get them to work to communicate from point "A" to point "B" We also have a group out

PL 86-36/50 USC 3605

there I call customers They're the service people who are thinking into the future what they want to dc, how they want to communicate, what's [sic] their network structures going to be In my career here I have not had enough dialogue with the people who are thinking about the future communication networks--the future communication systems That's the group I think we need to get better contact with and build some better bridges with Right now, I'm still seeing the services come in, saying, "We've got this architecture We're happy the way the system performs without crypto, but it has to protect classified information So would you please come in and add your crypto to it And, oh, by the way, it's got to be very small in size, weight, power and cost " That's okay, but when we do add our cryptography into it, we do modify the system parameters System performance can't change And if I start changing the system performance, then you're going to have a problem with the services--'cause they'll be disappointed with it "Yes, we ran all these great tests We liked it when it was passing in the plaintext But now I'm having a harder time communicating I'm getting more static in my lines I'm having more errors come through my data It's just not a comfortable feeling " And that's because the crypto is in there modifying the parameters So when If we can find out more of what they're doing, where they want to go five to ten years down the road--preferably ten years and out--we can start modifying our architectures of the equipment today, telling them where (B% their) system performance parameters impacts will occur A recent example has to do with the crypto-modernization They came to us and said wanted to know why they had to upgrade the cryptography [We] Explained to them all the rationale why They understood And they went away and they came back about three months later, said, "We've briefed the captain in the Navy We've briefed the admiral They understand the problem They're willing to sign on board We think it going to cost about sixty to seventy million dollars to do the retrofit of the equipment, and they're willing to buy into it " So we had some further discussions And in doing that, they had made a couple of mistakes in some assumptions they made because they did not understand the cryptographic properties When I explained to them the impacts to their system because of cryptographic properties, the bill went up to about eight hundred million dollars They couldn't afford it, so they had to put that on hold for a couple of years while they went ahead and figured out how they could tie that into their normal production rollovers for their equipment in the system Those are the kinds of impacts I'm thinking of If we can talk better to the get more information or better information from the people doing the planning of how they're going to communicate in the future, we could make changes to their system performance to accommodate some of the cryptographic problems or ((Slight pause)) Yeah, I can't think of the word right now the characteristics of the cryptography, take advantage of it, not have it show up as a problem in the system Because right now, a lot of times they'll come back and say,

PL 86-36/50 USC 3605

"Well, I got great quality when 'm not encrypted But when I encrypt it, the quality goes . . decreases."

Cooley: Mmm hmm

[redacted] "We need to have the quality the same." And it's not the fact we need to make their plaintext quality poorer, we need to make the crypto better And that means understanding their system and being able to maybe make some minor changes to the system performance--which they won't notice but would, in fact, improve the cryptography's performance in the system

Cooley: Okay, good Is there any final comment you'd like to make?

[redacted] Only final comment is I had a great career here We have a great workforce It's been fun It's been challenging And anybody who ever comes here could never say they've . . they had a dull or boring assignment for their career--because it only takes a little looking around to find a great assignment that would be challenging And it's one of the things I've always loved about this place the challenges and it's never boring There's always something new, different and interesting coming along--whether it be the space world . . You get tired of working space after a while, go work combat applications for the Army If you don't like that, you can go work with the Navy on some of the nuclear command and control ((He chuckles)) There's always something new and interesting You got your latest networks coming in

Cooley: Okay

[redacted] So it's been great

Cooley: Great Well [redacted] we thank you for taking the time to come down, and wish you the best of luck in your retirement

[redacted] Thank you

Cooley: Alright, thank you ((TR NOTE Audio ends here))

[redacted] PL 86-36/50 USC 3605 XXXXXXXXXXEND OF TRANSCRIPTXXXXXXXXXX