

DISCLAIMER

UNITED STATES NUCLEAR REGULATORY COMMISSION'S ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

The contents of this transcript of the proceeding of the United States Nuclear Regulatory Commission Advisory Committee on Reactor Safeguards, as reported herein, is a record of the discussions recorded at the meeting.

This transcript has not been reviewed, corrected, and edited, and it may contain inaccuracies.

Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

Title: Advisory Committee on Reactor Safeguards
 Digital Instrumentation and Control Systems
 Subcommittee: OPEN SESSION

Docket Number: (n/a)

Location: Rockville, Maryland

Date: Friday, October 23, 2009

Work Order No.: NRC-3162

Pages 1-20

NEAL R. GROSS AND CO., INC.
Court Reporters and Transcribers
1323 Rhode Island Avenue, N.W.
Washington, D.C. 20005
(202) 234-4433

UNITED STATES OF AMERICA
NUCLEAR REGULATORY COMMISSION

+ + + + +

ADVISORY COMMITTEE ON REACTOR SAFEGUARD

(ACRS)

+ + + + +

DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS

SUBCOMMITTEE

+ + + + +

OPEN SESSION

+ + + + +

FRIDAY

OCTOBER 23, 2009

+ + + + +

ROCKVILLE, MARYLAND

+ + + + +

The Subcommittee met at the Nuclear
Regulatory Commission, Two White Flint North, Room
T2B3, 11545 Rockville Pike, at 8:30 a.m., Dr. George
Apostolakis, Chairman, presiding.

SUBCOMMITTEE MEMBERS PRESENT:

GEORGE APOSTOLAKIS, Chairman

DENNIS C. BLEY

JOHN D. SIEBER

JOHN W. STETKAR

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

CONSULTANTS TO THE SUBCOMMITTEE PRESENT:

EARL BOEBERT

SERGIO GUARRO

NRC STAFF PRESENT:

CHRISTINA ANTONESCU, Designated Federal Official and
Cognizant Staff Engineer

CRAIG ERLANGER

RALPH COSTELLO

RUSS SYDNOR

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

T-A-B-L-E O-F C-O-N-T-E-N-T-S

Introduction.....	4
Cyber Security Assessment Team.....	8

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

P-R-O-C-E-E-D-I-N-G-S

8:28 a.m.

CHAIRMAN APOSTOLAKIS: The meeting will now to come order.

This is a meeting of the Digital Instrumentation and Control Systems Subcommittee of the ACRS. I am George Apostolakis, Chairman of the Subcommittee.

ACRS members in attendance are Dennis Bley, John Stetkar and Jack Sieber.

Sergio Guarro and Earl Boebert are also attending as consultants for the Subcommittee.

Christina Antonescu of the ACRS staff is a Designated Federal Official for this meeting.

The purpose of this meeting is to discuss Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities. We will also discuss the status of the Cyber security Assessment Team and the NERC/FERC MOU.

Any other acronyms, Christina?

CHAIRMAN APOSTOLAKIS: ACRS, GEA.

The Subcommittee will gather information, analyze relevant issues and facts and formulate and propose positions and actions as appropriate for deliberation by the full Committee.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 The rules for participation in today's
2 meeting have been announced as part of the notice of
3 this meeting previously published in the *Federal*
4 *Register* on October 1st, 2009.

5 We have receive no written comments or
6 requests for time to make oral statement from members
7 of the public regarding today's meeting.

8 A portion of this meeting may be closed
9 in order to discuss and protect information
10 classified as national security information as well
11 as safeguards information pursuant to 5 USC
12 55.2(b)(c)(1) and (3).

13 We also have Region II on the bridge
14 phone listening to the discussions. To preclude
15 interaction of the meeting the phone line will be
16 placed on listen-in mode during the presentations and
17 Committee discussions.

18 A transcript of the meeting is being kept
19 and will be made available as stated in the *Federal*
20 *Register* notice. Therefore, we request that
21 participants in this meeting use the microphones
22 located throughout the meeting room when addressing
23 the Subcommittee. The participants should first
24 identify themselves and speak with sufficient clarity
25 and volume so that they may be readily heard.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 Before we proceed with the meeting I
2 would like to welcome our new consultant, Mr. Earl
3 Boebert. And I would like him to say a few words of
4 why he's here.

5 MR. BOEBERT: I'm here because George
6 asked me to come.

7 CHAIRMAN APOSTOLAKIS: Okay.

8 MR. BOEBERT: He's a friendly guy, so you
9 know. George asked me to recite a bit of my
10 background. Air Force 1962 to 1966. Honeywell 1966
11 to roughly 1985. Technical founder of Secure
12 Computing Corporation, Sandia National Laboratories
13 from 1995 to 2005 performing intelligence analysis
14 and leading Red Team activities.

15 CHAIRMAN APOSTOLAKIS: Wonderful. Thank
16 you very much, Earl.

17 We'll now proceed with the meeting. I
18 call upon Mr. Craig Erlanger, Chief of the Integrated
19 Security Coordination and Policy Branch, Division of
20 Security Policy in the office of Nuclear Security and
21 Incident Response to provide some introductory
22 remarks.

23 Craig?

24 MR. ERLANGER: Good morning, everyone.

25 My name is Craig Erlanger, I'm the Chief

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 of the Integrated Security Coordination and Policy
2 Branch. And my branch is responsible for the
3 development of Regulatory Guide 5.71.

4 This morning, as was mentioned, we have a
5 very packed agenda with open and closed sessions.
6 We're going to begin with an overview of the Cyber
7 security Assessment Team, followed by a break to make
8 this a closed session. A very quick break. And then
9 we're going to be discussing the FERC/NERC MOU as
10 well as a detailed opening of where we have been and
11 where we are heading with cyber security regulations
12 throughout the Agency, given by my boss, the Deputy
13 Director for Reactor Security Scott Morris.

14 It's interesting to note that 5.71 is the
15 last of the tier 1 Reg. Guides related to the Part 73
16 rulemaking. So there is an emphasis states to get
17 this Reg. Guide completed. And we are really looking
18 forward to your feedback on your review of the
19 document, and hopefully answering any questions you
20 have related to the Guide.

21 With no further introductions, I'd like
22 to turn it over to Mr. Ralph Costello from the
23 Division of Security Operations. And he will be
24 providing you with an update on the Cyber security
25 Assessment Team. And if there are no questions, I

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 will turn it over to Ralph right now.

2 MR. COSTELLO: Good morning, everyone.
3 My name is Ralph Costello. I'm with the Office of
4 Nuclear Security and Incident Response.

5 I would like to thank the Chairman and
6 the Committee for the opportunity to speak here
7 today.

8 The purpose of my presentation is
9 information only. I'll be discussing the Nuclear
10 Regulatory Commission's Cyber Assessment Team, in
11 particular I'll provide an overview of the team's
12 formation and composition. I'll also discuss the
13 team's purpose, the progress we made to date and our
14 path forward.

15 The Cyber Assessment Team was formed by
16 the Executive Director for Operations of the Nuclear
17 Regulatory Commission in April of 2009.

18 The team is composed of staff with
19 expertise in cyber security from various offices and
20 regions. And the skills and backgrounds of the team
21 members are extensive and include digital
22 instrumentation and control, plant operations,
23 electrical information, technology security, digital
24 forensics, digital security and much, much more.
25 With this diverse and multi-talented group the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 Nuclear Regulatory Commission has the capability to
2 quickly marshall these skill sets to address any
3 emerging issues with potential cyber security related
4 implications.

5 The purpose of the team is to provide a
6 constant process for evaluation and resolution of
7 these events. I'm going to go over the process
8 briefly in the high level, and then on the next slide
9 I'll go into some more detail.

10 The first step that the team takes would
11 be to analyze and determine the facts; who, what,
12 when, where, how and why of the issues brought to
13 them. One of the first two questions we're going to
14 ask in that analysis phase is there an actual
15 perceived threat our licensees. And the other
16 question we'd want an answer to is is there a
17 vulnerability which can possibly be exploited by an
18 adversary.

19 The next thing we'd want to do is
20 determine the impact to our licensees.

21 And last but not least, provide
22 recommendations and services to our stakeholders.

23 The visual provided has the activity in
24 terms of how we process. And I don't want to belabor
25 a lot of detail here, but I want to give you a high

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 level view of how the process is going to work.

2 You can see that the slide provides two
3 columns. One column has the heading of threat on the
4 top, and the other column has the heading of event or
5 vulnerability at the top.

6 The first type I'd like to discuss of an
7 issue that would come to us would be one in which
8 there was a threat actual perceived to our licensees.

9 An example would be the Department of Homeland
10 Security United States Computer Emergency Response
11 Team provides an announcement concerning a certain
12 software vulnerability which would impact or could
13 impact our licensees. That would be processed
14 definitively by our Cyber Assessment Team, and again
15 using the overall high level processing analysis that
16 we have discussed, we'd look at the impact to our
17 licensees and provide recommendations.

18 The column on the left hand side gives us
19 an overview of those issues which at first we have an
20 unknown source of the issue. An example of that would
21 be a situation whereby a software anomaly could cause
22 a plant transient. Again, the initial cause were
23 unknown, and could have been possibly caused by
24 malicious actions. And because it's unknown, or
25 because of the capability of possibility errors, our

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 assessment team would process it through our system
2 and come to a resolution.

3 Again, we would want to have answers to
4 the following information:

5 We would want know is the issue caused by
6 an adversary, or possibly caused by an adversary
7 and/or is it a vulnerability which could be exploited
8 by an adversary threat. If the answer is yes to
9 either of the above, we would follow through to
10 final completion of our process.

11 CHAIRMAN APOSTOLAKIS: What kind of
12 guidance dose this team have? I mean, when you say
13 cyber team perform emergency assessment and so --

14 MR. COSTELLO: Yes.

15 CHAIRMAN APOSTOLAKIS: Does the team rely
16 on the expertise of its members or there is some sort
17 of guidance?

18 MR. COSTELLO: That's a very good
19 question, sir. You're reading into my next slide.

20 CHAIRMAN APOSTOLAKIS: I am?

21 MR. COSTELLO: Yes, sir.

22 CHAIRMAN APOSTOLAKIS: I do know that.

23 CHAIRMAN APOSTOLAKIS: Yes, sir. And I
24 appreciate that reading.

25 CHAIRMAN APOSTOLAKIS: Okay. Sorry. If

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 you are going to addressing it, that's fine.

2 MR. COSTELLO: I will.

3 I just want to add one more point. And
4 that is if the issue definitively not a vulnerability
5 or potential vulnerability and definitively not an
6 actual attack or an exploit by an adversary, then
7 obviously it would be handled through the normal
8 processes the Agency uses for digital I&C or
9 electricity for Office of Nuclear Reactor Regulation
10 and their processes, operating experience, et cetera.

11 I'll now follow into the Chairman's
12 question, this goes to the progress that we've made
13 so far. And we've developed a charter and
14 procedures. And as an answer to the Chairman's
15 question, we follow those procedures and we do rely
16 on the extensive backgrounds of the team members,
17 both here at Headquarters and the regions.

18 These guidelines are not set in stone.
19 We're Constantly enhancing them and improving them.
20 And as we speak we're making some enhancement to the
21 procedures as a learning and improving organization.

22 CHAIRMAN APOSTOLAKIS: I mean, again,
23 maybe it's because I'm not an expert in the field but
24 how do you decide what is a threat? It says here on
25 the previous slide threat or exploit. How does the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 team become aware of the fact that there is a threat
2 somewhere? I mean --

3 MR. COSTELLO: Well, the example I gave
4 was a US-CERT announcement of, say, a certain
5 exploit--

6 CHAIRMAN APOSTOLAKIS: Oh, so somebody
7 else tells you there is a threat.

8 MR. COSTELLO: There's many inputs. An
9 input can be from a licensee. Input could be from
10 US-CERT. Input could be through intelligence
11 channels. There's many input points that we view
12 this information.

13 CHAIRMAN APOSTOLAKIS: All right.

14 MR. COSTELLO: It could be an allegation.
15 There's other areas. I'm sure I'm missing where we
16 could have input points.

17 And then we would analyze them. We would
18 do a thorough analyses and we'd follow at the ground
19 to ensure that the public health and safety and
20 security is protected.

21 CHAIRMAN APOSTOLAKIS: Yes. Thank you.

22 MR. COSTELLO: As I mentioned, we have
23 these processes and procedures. And this team is on
24 call 24 hours a day, seven days a week and has been
25 since shortly after we formed.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 Have been trained initially in
2 conjunction with our Operation Center officers and
3 our Information Assessment Team. I'd like to say a
4 little bit about Information Assessment Team. You
5 may not know what that organization is, but they are
6 formed by intelligence analysts who have close
7 contact and integration with our partners in the
8 intelligence community. And we work closely with that
9 team also.

10 The training that we conducted initially
11 consist of: familiarization with emergency
12 operations; our procedures, as mentioned; digital I&C
13 controls, and; plant operations and scenario-based
14 team training. These joint training sessions that we
15 conduct initially we found to be very beneficial. We
16 will continue to this and other type training in the
17 future on a regular basis.

18 MEMBER STETKAR: Ralph?

19 MR. COSTELLO: Yes, sir.

20 MEMBER STETKAR: In your evaluations do
21 you make any attempts to rank or rate a particular
22 threat or vulnerability with respect to its relative
23 importance to plant safety, or is everything simply
24 rated a potential threat?

25 MR. COSTELLO: No. Your question is a

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 very good one. That is, in fact, one of the
2 enhancements we're making to the procedure as we
3 speak. So that, we found out very early on that that
4 would be a very good tool for the team to
5 expeditiously process and know where to go. And
6 these are all learning things that we found out real
7 early on, and that's part of the --

8 MEMBER STETKAR: It's in process right
9 now?

10 MR. COSTELLO: It's being integrated in
11 the procedure as we speak. And it's going to be on a
12 color-based tiered level.

13 MEMBER STETKAR: So it seems to work, so
14 that's fine.

15 MR. COSTELLO: Sir?

16 MEMBER BLEY: That guidance is going to
17 be in the new ISG when we see it, is that right?

18 MR. COSTELLO: I don't believe it will
19 be.

20 MEMBER BLEY: It won't? It's separate?

21 MR. COSTELLO: Yes, sir.

22 MEMBER BLEY: I was just curious.

23 The ISG, I guess I get mixed up on this
24 occasionally. The ISG can either be something that's
25 going to become an SRP or a Reg. Guide. And the ISGs

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 here are aimed at the Reg. Guides, is that right
2 rather than SRP?

3 If this is going to be guidance to your
4 staff, why wouldn't be in an ISG or a SRP?

5 MR. ERLANGER: What might be helpful is
6 how the CAT team came into existence. We were under
7 direction from the EDO to come under the process to
8 deal with everything Ralph mentioned and in addition,
9 the topics you saw on the news. The Soviets attacked
10 at Georgia, the Chinese attacked the grid.
11 Everything, how do we address and deal with these
12 issues.

13 What we're in right now is a one year
14 pilot to conclude approximately winter of 2010. So
15 at this time we're basically just trying -- we
16 recognized a need to deal with an emerging threat, a
17 topic that was constantly in the news. You caught
18 all these headlines. There were a few just this week
19 that we saw there. How do you take that, what you see
20 in the news, or a real threat that we get through
21 intelligence channels and work it into our
22 longstanding processes. The analogy that Ralph made
23 to the Information Assessment Team is probably the
24 closest.

25 As you know, 24/7 you might have an

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 incident at a plant related to, it could be a pipe,
2 it could be whatever and there are subject matter
3 experts available to look at that to adjudicate it
4 whether it is a just it happened because or there was
5 some malicious intent. So that's what this process
6 is trying to mirror.

7 Whether or not it fits into an ISG or
8 Reg. Guide, I would say that is not the thought
9 process at this time. It's just really --

10 CHAIRMAN APOSTOLAKIS: But what you're
11 doing today is just briefing the Subcommittee.

12 MR. COSTELLO: Yes, sir. Just information
13 only.

14 CHAIRMAN APOSTOLAKIS: That this team
15 exists.

16 MR. COSTELLO: Absolutely, sir.

17 CHAIRMAN APOSTOLAKIS: It has nothing to
18 do with Regulatory Guide 5.71?

19 MR. COSTELLO: It is not. That's correct,
20 yes.

21 MR. ERLANGER: That's correct.

22 CHAIRMAN APOSTOLAKIS: This is he warm-up
23 performance?

24 MR. COSTELLO: It's background
25 information that --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CHAIRMAN APOSTOLAKIS: The warm-up.

2 MR. COSTELLO: -- we feel you need to
3 know.

4 MR. ERLANGER: It's another leg to what
5 we're doing for cyber as an Agency.

6 CONSULTANT BOEBERT: How many people?

7 MR. COSTELLO: Over 20.

8 CONSULTANT BOEBERT: How many locations?

9 MR. COSTELLO: Headquarters and the four
10 regions.

11 CONSULTANT BOEBERT: Communications,
12 secure mail --

13 MR. COSTELLO: We have all that. Yes,
14 sir.

15 CHAIRMAN APOSTOLAKIS: Okay.

16 MR. COSTELLO: And last but not least, we
17 can open the database with current and past notable
18 issues as a tool for this team to work through its
19 issues.

20 The path forward.

21 As noted previously, we're going to
22 continue to assess team processes as noted by the
23 some questions we've already worked towards, some of
24 those improvements already.

25 And we're going to apply those

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 efficiencies through enhancements on a continuous
2 basis and, obviously, continue training efforts in
3 that vein.

4 Today we discussed the Cyber Assessment
5 Team's formation, the composition, the team's
6 purpose, the progress we've made and our path
7 forward. Are there any questions?

8 CHAIRMAN APOSTOLAKIS: Well hearing none,
9 thank you.

10 MR. COSTELLO: Thank you, sir.

11 CHAIRMAN APOSTOLAKIS: We're ahead of
12 schedule here, aren't we?

13 MR. COSTELLO: I'm sorry about that.

14 CHAIRMAN APOSTOLAKIS: Yes, you should
15 apologize.

16 Now we're moving to Mr. Morris, or he's
17 not here.

18 MR. SYDNOR: He stepped out to his
19 office?

20 CHAIRMAN APOSTOLAKIS: Russ?

21 MR. ERLANGER: Let me, I'll grab him.
22 He's probably right out this door.

23 MS. ANTONESCU: We're moving to the
24 closed session?

25 CHAIRMAN APOSTOLAKIS: Who is?

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MS. ANTONESCU: Well, we are.

2 CHAIRMAN APOSTOLAKIS: Yes, you're right.

3 Okay. So what do we do?

4 I am advised that we are moving to a
5 closed session. And, Christina, what does that mean?

6 MS. ANTONESCU: That means that people
7 who were already approved are able stay, and the
8 other ones have to leave the closed session.

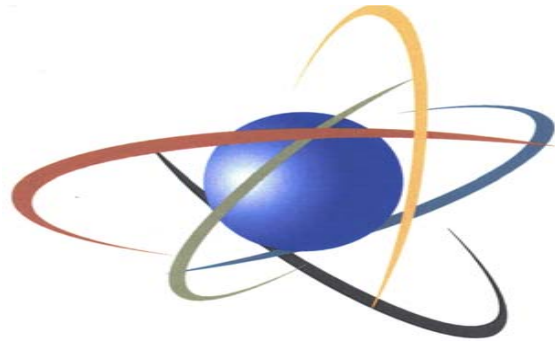
9 (Whereupon, at 8:48 a.m. the open session
10 was concluded.)
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701



U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

NRC CYBER ASSESSMENT TEAM

**Advisory Committee on Reactor Safeguards
Digital Instrumentation and Control Subcommittee
October 23, 2009**

**Ralph Costello
Division of Security Operations
Office of Nuclear Security and Incident Response
(301-415-6821, ralph.costello@nrc.gov)**



Formation of the CAT Team

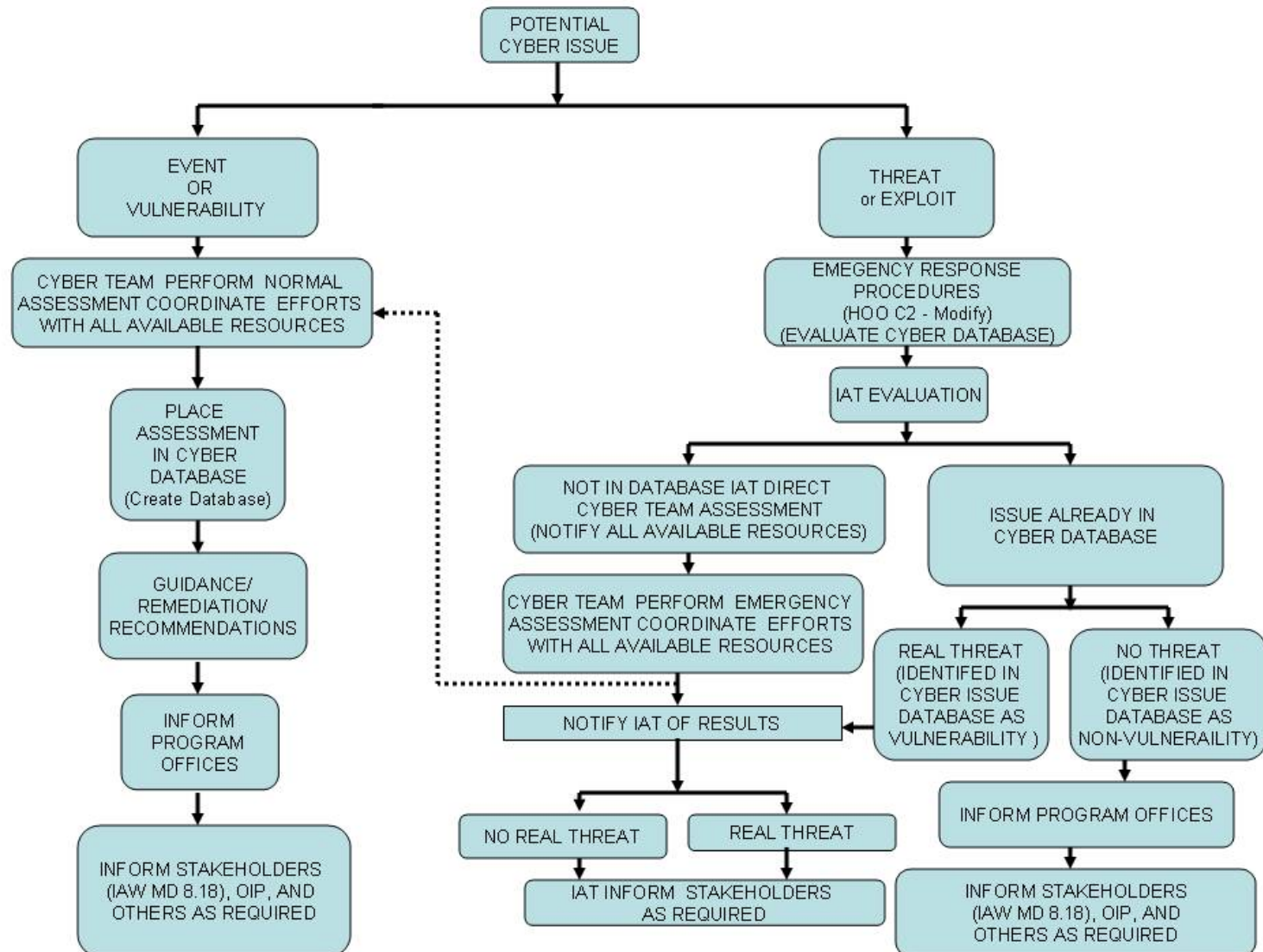
- **CAT team was formed in April 2009**
- **Composition of the CAT team**



Purpose and Process

- **Provide a consistent process for evaluation and resolution of cyber security issues with potential cyber security related implications**
- **Process**
 - **Analyze cyber security issue**
 - **Determine the facts**
 - **Determine impact to licensees**
 - **Make recommendations to stakeholders**

Process continued





CAT Team Progress

- **CAT team charter and procedures**
- **Cat team is available on a 24/7 basis**
- **Personnel have received initial training**
 - Regular continuous training
- **Database is being developed**



Path forward

- **Assess processes of the CAT team**
- **Apply enhancements - continuous**
- **Continuous training**



Questions?



Acronyms

- **CAT – Cyber Assessment Team**
- **HOO – Headquarters Operations Officer**
- **IAT – Information Assessment Team**
- **IAW – In Accordance With**
- **OIP – Office of International Programs**