File 20110801.0900 (CDT): Notes from UCDMO conference sessions:

Exhibit spaces are setting up Monday and not generally accessible until tomorrow. Open Tuesday and Wednesday, tearing down Thursday.

0900 Cross Domain Technical Forum (CDTF), introduced by Angie Moser, NSA/I22311 chief. All sessions are unclassified/FOUO. Five Eyes partners are present. NSA is naming their departments after ZIP codes now. This morning's session is about CDS and where we need to go as far as development.

James Garriss, MITRE, on 'HTML Inspection and Sanitisation Guidance (ISG)'. There were more than 107 trillion emails sent last year, almost 97 percent of which used HTML formatting. ISG identifies potential risk areas: data hiding, data disclosure, and data attacks. ISG provides multiple recommendations.

Static HTML ISG: concerned about sensitive information in the attributes of HTML that render nothing visible to the user. Possible to neuter URLs by inserting the word DENIED into a link to distrupt DNS resolution. Height and width attributes may be set to ero by attackers to hide images; the CDS can reset them to a default value like 200 pixels. HTML can contain comments. NSA working on a new ISG solely about Javascript. Discussion of removing HTML FORM elements. Attackers might set the 'disabled' attribute on FORM elements to hide information; if the CDS removes the 'disabled' attribute, the information in the hidden FORM elements will be visible to a user. The HTML OBJECT element is similar to EMBED. It is possible to hide data in NOSCRIPT elements. The DATA URI Scheme allows embedding content directly in HTML, usually Base64 encoded, but this is not required by the spec.

Dynamic HTML ISG: Javascript is the key enabler. Attack surface greatly expanded: database storage, socket and file I/O, 2D and 3D graphics, animation, encryption, validation, DOM, math, the semantic web. Example: an HTML 5 canvas document.

Assertion: it is impossible for reliable human review or a computer programme to detect all the myriad ways of hiding information in a canvas. Burn-ins, etc.

NSA's HTML Filter 1.0—identify and sanitise. Using FCE: Filter Componentisation Effort. Available in October 2011.

Status: Static HTML ISG is nearly done except for HTML 5. Dynamic HTML ISG is not as far along. CSS ISG handles CSS 2.1 but needs CSS 3 and Javascript.

Ask Boyd Fletcher or Sheree Elliott for an account if you want the ISGs. Email: `boyd.fletcher@us.army.mil` NSA/I22311 or `snellio@nsa.gov` NSA/I22311 or James Gariss `jgarriss@mitre.org` or NSA, Cross Domain Solutions, I22311.

0955 Matt Kochan, DoDIIS CDMO `matthew.kochan@rl.af.mil` on 'C-SCOPE: Centralised Secure CDS Observation to Protect the Enterprise'.

There is not enough situational awareness of our CDSes. Lacking good remote monitoring/remote administration; limited diagnostic information; KVM over IP is state of the art right now.

'CD engineers are making CDS solution decisions without knowledge of capacity status of candidate solutions.'

Service providers lack detailed knowledge of CD transactions specific to a customer that could be used for CDS usage billing.

Feedback to users on the success/failure of their individual CDS transactions is insufficient and causes delays in transfers, unncessary re-sends, inefficiency, and frustration.

CSCOPE in a nutshell: developing and fielding of an initial pilot of a CDS operational Health and Status Monitoring (HSM) dashboard within DIA.

We know we lack CDS SA; some CDSes are already reporting SNMP MIB information, but MIB compliance has not widely taken root yet.

Development in FY 11/12; fielding pilot in Spring 2012.

Dashboard will monitor ISSE and RM systems at SE-SRC (Tampa) and NE-RSC (DC area) and one other SRC.

SNMP MIB is critical because they are hopeful of avoiding a new C&A, 'which we can ill afford'.

Core targeted capabilities: stoplights (red, yellow, and green); tie utilitisation statistics to the inventory database for capacity planning and implementation of pay-as-you-go usage billing.

Stakeholders: DIA enterprise operations management; DCDMO enterprise operations/solutions engineering; CDS programme offices; CDS admins and managers. They polled all the stakeholders and got feedback from them.

Other RSCs: SE-RSC, WC-RSC, EURSC, PA-RSC, NE-RSC.

Functional architecture diagram: log, collect, transfer/parse, store, and visualise.

Physical architecture: CDSes send data over JWICS to server, then it is visualised from the server.

CDS SNMP MIB compliance: of 145 elements identified by the CDS MIB, Radiant Mercury implements 44, or 30 percent; ISSE implements 34, or 23 percent; and common to both Radiant Mercury and ISSE are only 28, or 19 percent of all CDS MIBs.

Much of the data they want is in the CDS logs already in textual form, but needs to be exported in the form of SNMP MIBs. Suggestions for MIB updates: (1) report the actual size on disk of each audit file, along with limits; (2) list of all possible alarm types; (3) more details on thread errors; (4) summary of the last n configuration changes; (5) please report numbers in floating point, not the older and more limited traditional fixed decimal format.

Usa cases: they would like guards to be configured in such a way as to track individual customer usage within aggregated data flows, which today might be feeding dozens or hundreds or thousands of customers out in the field. They want to be able to bill each of those customers for their own individual CDS usage.

Roadmap: pilot in 2012 using RM 5.0 and ISSE 3.6/4.0; identify shortfalls in HSM info. Deployed system in 2013–14 with additional CDSes, additional views and reports and alerts, leveraging SNMP MIBs. Advanced models in 2015 and beyond with more drill-down capability, more use of knowledge base.

1045 Larry Brown on 'Lessons Learnt Integrating SNMP':

It is Radiant Mercury's 20th anniversary. We have been inventing these things as we went along because we saw the need for them.

Current situation: the CDS administrator must walk to a computer room or server closet or login with a browser to get status information from the CDS.

SNMPv3 gives us continuous status monitoring, provided remotely, standardisation amongst guard vendors, a freely available monitoring agent, and is part of RM's roadmap.

Cross Domain SNMPv3: by definition, the net manager and managed devices reside in different domains.

Option 1: RM acts as a transparent proxy; it must read packets off the wire in promiscuous mode because the packets are not addressed to us. RM does SNMPv3 authentication, validates headers, parses the ASN.1 and validates OIDs within. Initially, we used MAG for this, but now use the SNMP4J library.

Option 2: RM sits between two dedicated Network Managers talking XML to each other through the guard. Disadvantages: requires more rack space. Advantages: SNMPv1 and SNMPv2 are supported, configurations can be installed via DFCF, and it uses COTS XML for parsing.

Experiences using RM to emulate an SNMP agent: allows net manager to query RM's own status; RM can send out its own traps, too; RM authenticates SNMPv3 header using SNMP4J using the same mechanism as CD transfer; supports a small subset of the CDS MIB, but it is extensible; pre-dates the CDTF MIB.

New approach: integrating freely available NetSNMP agent. There are two versions of NetSNMP agent: an NSA sponsored version specifically for CDS that offers read-only operation, and notification only operation with no 'set' or 'query' commands supported, a reduced code base for security review (provided via command-line switches), and a very responsive developer in the person of Wes Hardaker. He always provides quick responses when the RM developer has questions. There is also the full-featured version of NetSNMP available for downloading off the net, of course.

Current integration status: requirements analysis is done and inspected. Prototype tested with the Cacti Net Manager and NetSNMP command line utilities. Initial support on IPv4 only; deferring testing of IPv6 and datalink until later. Security mechanisms implemented: SNMPv3 authentication and privacy, user access limited to a defined subtree of the MIB, and use of out-of-band communication to the Network Manager.

Working with Solaris Zones, the status daemon runs in the Global Zone aling with the SNMP sub-agent. SNMP master agent runs in a SYSHI zone. All external SNMP communications take place to the SYSHI zone only.

Implementation issues: static vs dynamic data; traps vs gets (gets are good for polling); gets are probably more useful for trending; use of crontab for firing off periodic traps at configurable intervals; should we cache status updates, or collect status only on demand?

How to populate OIDs with RM status: text based status is available already, and covers most of the dynamic data required by the CDS MIB OIDs. We use a phased approach: first implement the required OIDs, followed by the optional OIDs, and finally RM unique extensions.

RM's role in DoDIIS C-SCOPE: RM and ISSE are early integrators with C-SCOPE. Pilot in CY 2012 on JWICS. Dashboard server provides text to SNMP translator. Compatible with RM 5.0 and other certified guards.

Example of system and communication status: reports unique message ID, system time, process size (useful for detecting memory leaks after it reaches stable operation), CPU time used per message, channel type, number of state changes, channel name, port number, total run time of the process, and so on.

1130 Boyd Fletcher on JALoP (pronounced 'jalopy'). Auditing, logging, and journaling.

Audit messages fit nicely into enumerated type bins. Logging messages don't. There is no current protocol that can handle journaling messages. What to do, what to do?

Existing JAL protocols are insufficient, so they developed a new protocol called JALoP with an open source API, a daemon server process, an example repository, and 'data taps' to make it easy to try out on existing guards. Here's how it works:

There is a JALoP Network Protocol (JNP), and a JALoP Producer Protocol (JPP). The CDS writes JPP data to a JALoP network store, and then a JALoP network library talks JNP to the outside world.

CDS users hate to go to the CDS every couple of days to run backups. CDS configurations change seldom anyway, but logs accumulate rapidly. Store those logs off the CDS and you eliminate most of the backup problem of CDSes.

JNP uses an IETF protocol called BEEP: the Block Executable Exchange Protocol. BEEP guarantees in-order delivery, uses TLS for security on the wire, and has unlimited payload size. Structurally, BEEP looks a little like SNMP and a little like HTTP. It uses key–value pairs. It is a fully bidirectional protocol; either a repository or a producer can be an initiator—this lets you do some very cool things.

JNP record formats: audit record, or journal record, or log record.

Three mechanisms to protect the destination from malicious journal data: use deflate, or AES, or XOR. The reason is to protect against accidential execution of malicious data in log records from a CDS that detected the malicious data properly, logged it properly, and sent it to a stupid Microsoft Windows log server that stupidly viewed the log file and got itself infected. This has actually happened in the field. (An interesting security misuse case—I ought to point it out to Shamal.)

JPP: a simplified version of JNP. No BEEP framing, uses UNIX domain sockets; all fields are length limited, all payload is binary. It allows file descriptor passing for journal data; this lets the local store capture a 16 gigabyte file, for example, right off the disk without copying the whole mess of data through a UNIX domain socket unnecessarily.

Data Taps (these are cool). Provides a mechanism for CDS developers to quickly adopt JALoP without having to modify their applications at all. Data taps under development include Linux Audit (implemented as an audit dispatcher), GNU tee (implemented as a new command line option), GNU tail (implemented as a new command line option), rsyslogd (implemented as a plug-in; rsyslogd is the currently most popular remote syslog programme, replacing syslog-ng which has fallen out of favour lately), and Apache Log4C and Log4C++ (implemented as an appender). Future data taps will be developed for Solaris Audit, Apache Log4J, and others as requested.

Finally, the CDS CEE mapping. All guards currently use different terminology in their log messages. This is frustrating and is currently resolved by use of incredibly expensive log analysis tools. Recommend using MITRE's SCAP-based Common Event Expression (CEE) instead.

They researched audit/log events from most of the UCDMO baselined transfer CDSes to make a list of these. Niftily, CEE contains support for internationalisation built-in, in hopes of getting buy-in from commercial software developers; the English language format of, for example, a CEE type 12345 log message is defined in the CEE database with a bunch of replaceable formatted fields like a printf string in C. The only data that crosses the wire are the CEE event number 12345, the date, time, file names, etc. The message is automatically formatted and internationalised for display in whatever language the user wants to read it in.

For more information, `http://cee.mitre.org`.

1300: Dan Nichols on the 'High Robustness Cross Domain Solutions Tiger Team'

(Note: the next CDTF will take place April 2012 in the DC area.)

Dan Nichols is chair of the CSTG and several tiger teams. The high robustness CDS tiger team started about a year ago. Commercial products are typically low or medium robustness only. Estimate about 20 percent of CDS customer space is in the riskiest environments, and need high robustness.

Purpose: to establish common high robustness CDS terminology and definitions, HR CDS criteria.

Deliverables: a robustness scale, criteria for using HR CDS, requirements for HR CDS design.

They do not have a list of applicable NIST SP 800-53 security controls yet. They did not have enough resources to do that.

They did define the following documents: security objectives and security problem, low-level design, high-level design, and requirements.

Jennifer Guild, co-chair of the HR CDS Tiger Team: 'we narrowed down the HR problem away from Type 1.' CNSS 4009 defines assurance, but not robustness. Robustness may be defined as follows: 'the system behaves as expected no matter what happens'.

Example: Minuteman ICBM was HR before HR was cool. Not all silos contained missiles, because there were not enough missiles to go around. So information about which silos contained missiles at any given time was Top Secret. They managed to process TS and unclassified data on connected systems. So can we.

Correlated to System Security Engineering (SSE) Framework.

HR assessment requires analysis, not just testing. There must be a framework so that evidence pieces are reusable for other assessments later on.

It covers the life-cycle from mission needs statement to problem definition to solution realisation.

They defined a mapping, the SSE framework for high robustness.

Some security principles cannot really be tested—they are verifiable only through analysis. For example, least privilege, or domain isolation.

Security relevant functions are either security enforcing, security supporting, or security non-interfering. Security functions should be implemented using the security principles. For example, how do you prove that TSOL does object reuse correctly? By analysis. Must have security principles to even begin this analysis, and analysis is the only way to show it, because testing can't do it.

Security Problem document, Security Objective document, Security Policy document (first in an informal notation, then more formally).

You must identify all flows, including ones that should be prohibited. (This is relevant to Professor Irvine's later question about covert channel analysis.)

You should not specify mechanism.

Security Requirements document: a clear, unambiguous, and well defined description of the expected security behaviour of the system.

Security Architecture document: a combination of formal and information techniques that express the adequacy of the security mechanism.

High Level Design document: provides a description of security functions in terms of major structural units (i.e, subsystems) and relates these to the functions they provide.

Please send comments to Jennifer.Guild@navy.mil Tel. 843-218-4879. Looking for feedback from the community.

Comment from audience: 'I don't know whether I need an HR CDS because I don't know what the threat is. When I ask what the threat is, I am told it is classified above my clearance level.'

Response from Jennifer Guild: every HR implementation is a specific solution to a specific problem. Can't go into basic threats in an unclassified environment. Call me and we'll discuss it.

They are working with NIST to update 800-53 to include a chart for choosing a robustness level.

Question from audience: how much overlap is there with Common Criteria and NIAP? Answer: we took the best pieces from NIAP, the rainbow series, and DCID.

Question from Professor Cynthia Irvine, Naval Postgraduate School: is the CCA block on slide 13 missing a feedback arrow? Answer: oops, yes it is missing an arrow.

1415 High Robustness CDS Tiger Team Panel Discussion, including Dan Nichols, UCDMO and moderator; Professor George Dinold, Naval Postgraduate School; Jennifer Guild, SPAWAR; John Mildner, SPAWAR, and Thomas Macklin, NRL.

Note: Jennifer Guild sounds like a weapons officer. She wants HR CDS because missiles are connected to C&C networks that are not.

John Mildner: we need HR CDS because in some CDS applications, you have one and only one chance to get it right.

Thomas Macklin: there are several problems that HR CDSes can solve: they are resistant to the problems of software monocultures, and they avoid that I call the 'OMG' type problems, where you go in and tell a network manager that a new threat completely overwhelms all his defences: he just stands there with his mouth open and can't manage to say anything.

Prof. Dinolt: the requirement for robustness pervades things outside the government community; for example, automobile engine control computers, and cloud computing need HR too.

Question from audience: in the past, the way you did HR was that you built it, you gave it to NSA to play with for a while in the corner, then they came back and handed you the broken pieces and told you, 'nope' and they didn't tell you why. The orange book, the Common Criteria, NIAP, all of these were very process-oriented. Could you elaborate?

John Mildner: many of those processes are tail-end loaded. Our process is aimed at making sure the *appropriate* artefacts are delivered.

Thomas Macklin: we are trying to narrow down the problem from the old 'this is a C2 evaluation' or 'this is an EAL2 evaluation'.

Jennifer Guild: no more 3–5 year evaluations through the Common Criteria; all of us on the tiger team have used the rainbow series, we used the CC, so we are of course influenced by them.

Question from Professor Irvine: the current definition of HR includes resiliency. How are you to recognise it when you see it?

Professor Dinolt: we don't have resiliency in computing yet. The telephone company is closest to having it.

Jennifer Guild: we have good ideas why we need it. We know what it takes to be resilient against attack. How to measure resiliency, that's still a problem.

John Mildner: resiliency is a combination of integrity and availability, which requires provision of redundancy and automatic reconfiguration.

Thomas Macklin: acquisition people have no language at present to write resiliency into their RFPs.

Question from the audience: do you anticipate HR CDS solutions to be inherently GOTS?

Jennifer Guild: for embedded systems, we expect GOTS-modified COTS to be prevelant. For data centre applications, COTS.

John Mildner: I'll offer my standard security answer: 'it depends'. But the government does not have the capacity to develop it all itself.

Question from MITRE: to what level will formal modeling be used?

Professor Dinolt: at present there is a lot of formal modeling happening in hardware development. What is missing is an understanding of the security properties of the chips for isolation and domain separation. I hope that researchers in future will do more on that.

Thomas Macklin: for example, cache and other familiar features of our hardware today would not exist without formal modeling. It is used, just not so much in the security area now.

John Mildner: languages for formal modeling tend to get used on security critical code only.

Jennifer Guild: most of the formal modeling people in in the United States are over the age of 55. This is less true in the UK, Canada, and Australia, but it is here. Don't think that formal modeling is used only for security; there is lots of use in aircraft, both civilian and military, for safety critical systems. The U.S. needs more formal modeling experts, and we're not growing enough of them.

The HR CDS TT needs feedback from two groups: from the user community and from the acquisition community.

Question from the audience about HR on commodity hardware.

Jennifer Guild: almost all HR is already done on commodity hardware. With one exception, all HR CDS development to date had been on commodity hardware. We do not specify mechanism, only functionality and policy.

Question from the audience: 'semantics are important. What are the real definitions of high robustness, resiliancy, and assurance?'

Jennifer Guild: the TT spent lots of time on semantics. We argued for hours over the inclusion of one word in a particular definition. '4009 should solve the problem.' [laughs]

Question from John Benner: how well defined is the process intended to be, and who is to pay the cost?

Jennifer Guild: we are not expecting twenty of these a year, only about five a year. For example, if I did a PL-5 guard, I know of people who spent 10 million dollars on a guard but had to throw it away. Under the new process, we are looking at maybe 1.5 million dollars, maybe two million, because we embed SMEs from the beginning.

John Mildner: complex IT systems have a dismal success rate, irrespective of security problems.

Thomas Macklin: at last year's UCDMO conference, statistics were presented that showed only a minuscule percentage of systems failed due to security requirements. They failed for other reasons.

Question from the Boeing Company: reflect upon systems that came before: the rainbow series claimed that any system wanting to be HR must be MLS. And the evaluators were deeply involved. The along came the Common Criteria, and we called it validation rather than evaluation, and the validators wanted to do it faster and at lower cost. But the CC was overly flexible, it took too long, the validators were less involved in design, and they were more oriented to looking at evidence. How are your new processes going to take advantage of the best parts of the past?

Jennifer Guild: not full-time embedment of SMEs, but closer contact. Awareness of when design reviews are coming up. Using the best parts of the CC and the rainbow series. There is lots of experience on the Tiger Team with all the previous evaluation schemes. The TT wants feedback from the community.

The new process is designed to succeed more often than at present. It will have to be flexible to adapt to operational risk.

Question from the audience: how does operational test and evaluation fit in?

Thomas Macklin: we can't test until the system has been developed.

Jennifer Guild: requirements elicitation is like pulling teeth—have to go back to the users with the requirements and see if the requirements make sense to the users.

Comment from audience: you have to embed SMEs who are über geeks. They must truly understand the problem domain. Don't waste our time otherwise.

Jennifer Guild: we anticipate putting only one SME in, with wide and deep experience, and they won't be contractors. It will be a government-only function. (This seemed to satisfy the audience member who made the comment.)

Question from MITRE: what is the target of this process? Gate level hardware, software, or top level architecture?

Jennifer Guild: we don't have the process done yet. Draft process is still classified, has not been released yet. All of what we presented today was classified until last week. This is the first time it has been socialised. But it was written to apply to any level.

John Mildner: in the DCID 6/3 days, a PL-4 system was primarily PL-2 throughout most of it. There was just a small portion of the system that was PL-4.

Question from the Naval Postgraduate School: how will sites be able to maintain an HR CDS once it has been deployed?

Jennifer Guild: we will be cooperating with industry to keep up with changes in chip sets.

John Mildner: maintenance of ratings is the most personnel-expensive phase of any evaluation criteria.

Question from the audience: do you have a timeline for rolling all this out?

Dan Nichols: today is the first time this TT's work has been socialised. We are looking for feedback from the community. The DISN Flag Panel is the next place this is going to be socialised at.

Question from the audience: is this the new home of high robustness?

Jennifer Guild: the official answer is that UCDMO is responsible for all CDS. The TT is working with NIST, NSA, and UCDMO.

Question from the audience: what about NIAP?

Jennifer Guild: can't answer that.

Question from the audience: do you see a time when the DSAWG or DoDIIS will say, 'this needs an HR CDS'?

Jennifer Guild: the decision cannot be left up to the customers. Evaluators must have a say, also accreditors, customers, even the operators.

Question from Karen Burke, NPS: how will customers recognise the need for HR when they can't even recognise the need for security today?

Jennifer Guild: 'education' is a bullet point on every slide we presented.

Comment from the Boeing Company: 'functionality trumps assurance every time'.

Jennifer Guild: 'operation trumps functionality every time'.

Comment from Professor Irvine, NPS: 'things have muddled along pretty well until now. Nothing bad has happened.'

Jennifer Guild: how do you know nothing bad has happened? Would Sony say nothing bad has happened?r What about the Estonian banks? I have heard examples of terrifying things I can't talk about here.

Dan Nichols: the baseline list is no longer a re-use list, it is a validated products list. UCDMO is helping in real ways.

Comment from the Boeing Company: need to educate the acquisitions people to write HR and resiliency into the contracts.

Jennifer Guild: need to give the security guys the ability to kill a programme. Otherwise you will not have real assurance. Many a CDS has been killed by Microsoft Windows. The users want their Microsoft Office. Open Office is not good enough. They want office. At present, they are getting it, and the CDS is losing the fight.

Question from the audience: what is UCDMO's approach to getting training down to the guys in the field?

Answer: not there yet.

Question from the audience regarding the Zumwalt programme: will the new process help the tail-loading of existing security processes?

Jennifer Guild: all the gotchas that got slammed on Zumwalt would have been caught by this new process ahead of time.

End of CDTF, 1600 Monday.

Notes from RM and TMAN kick-off meeting, room 677:

Steve Bean: we are looking for cross-pollination. Make an effort to learn both sides. Rather than bringing eight people next time, we could bring three who knew how to run all the demos.

Don't crowd the LM booth. If there are too many people there, go to the techical sessions, collect intelligence on our competitors in the exhibition.

Jeff Dutoit will be in the booth the whole time. Need other people to collect brochures from other booths. Discussion of whose faces are known to competitors and who are still anonymous.

Jeff pointed out that we could sell Probabilistic Redaction to all the other guard vendors.

Later this month, build a spreadsheet of intell on competitors. Gather their brochures.

Xmeridis (spelling?) is a competitor to TMAN. The Raytheon High Speed Guard is trying to eat DCGS. They bought TCS. Our competitors are: ISSE, Xmeridis (sp?), and Raytheon High Speed Guard.

Rumour: DII is replacing RM and TMAN across all the decks.

Olav: Oracle scares me. They are trying to price others out of the market be means of what they control access to.

Jeff: what about the General Dynamics Tactical CDS that 'uses MAG'?

Discussion of doing accreditation ourselves. All it is, is document preparation. We used to do it, according to Ernie. We didn't have Booz Allen doing IV&V. Larry disagrees; Booz Allen was there from the beginning. Ernie says they were doing testing, not IV&V.

Discussion of scanning badges to get contact information from attendees. Kim Frey says we didn't rent a barcode scanner because the cost is exorbitant. Conclusion: ask for business cards and write down contact information, stick them inside your badge holder.

Idea from Jeff: we should send out quarterly emails to remind people (like RMUG attendees) that we exist: 'save the date' kind of things.

Rumour: DIA might reorg and get rid of all their certifiers, pushing it all back out to the services.

Olav: want to have dinner Wednesday night. The speakers' reception is a conflict, however. Jeff Dutoit went to the speakers' reception last year, and notes that it was a very small event, but *all* the key players were there. Consensus that Larry ought to go to the speakers' reception; we will schedule dinner later so he can attend both.

Steve Bean: both TMAN and RM are below their numbers this year. Not just below the increased level expected, below last year. We need to sell product at this conference.

Ernie: Frank Sinkular wants to meet this evening to talk about FMS (see below).

References