File 20110802.0805 (CDT): UCDMO conference notes part 2.

0810 Frank Sinkular, acting director of UCDMO.

0815 Cheryl Roby, Chief of Staff, ASD(NII)/DoD CIO: the new norm is to always be in a coalition sharing environment. We need defensible networks. Coalition partners change. Not all coalition partners are equal; Five Eyes is one relationship, NATO is a different sort of relationship.

Metadata tagging is very important: NATO standards, national standards.

Imperatives: (1) enterprise, (2) cyber.

Recently, Deputy Secretary of Defence intoduced the Defence Strategy for Operations in Cyberspace, or DSOC. The pillars for operations in cyber environment: be proactive; protect networks.

The president put out US norms for operations in the international internet. Norms of behaviour for operating in cyberspace. We need to have this kind of norms: 'if you cross this line, that will happen'.

We have got to make Enterprise the main solution. Point-to-point is still important, but we must think about the enterprise.

Every day, a thousand CDs are being burned to share operational information in the tactical environment. Spills will happen. This is not the day job of people doing the war fighting; we throw complex COTS products at them with inadequate training. What tools can we put in their hands to automate the information sharing they need?

In Washington, they have unlimited bandwidth, a robust infrastructure, and lots of experts standing around ready to help. In the tactical environment, they have low to moderate bandwidth, insufficient resources, inadequate training. Must make that difference clear to the seniors in Washington.

Afghanistan Mission Network (AMN): a success story, sort of. It was built on the fly after the mission was already under way. The airplane was built in flight on the way to the fight.

Three stars and four stars are not getting it; 'CDS is key terrain' but where is the money for CDS? It's there, but it's buried, not obvious. It must be raised and reallocated, because there is no new funding.

Were are we now with CDS? (1) Configuration Management: we are not properly installing CDSes today. (2) System administrators of CDS are not well trained. (3) Maintenance of CDS is not well handled.

AMN is a manageable risk, but we need to get to enterprise.

What is different this time? For the first time, we have done an operational assessment of AMN and got it to the senior level.

Grades: in IT consolidation, give it a C. Enterprise services, B minus (we have an enterprise email system now, but it has all of 500 users on it).

One success story is VTC: NSA IAD and DISA set up a VTC system that allows US Secret VTC with coalition partners, and the VTC is well used.

Requirements processes, acquisition processes. Those were past successes. What is the future? Enterprise, scalable, and dynamic.

Networks operations must be reusable. It has got to be in the initial stages of planning.

Cyberspace: she mentioned the DSOC, focus on lessons learnt.

DoD CIO have a vision beyond point-to-point solutions, to the enterprise. But the enterprise must support the tactical user.

There are 800 people in this room. 'I give you a call to action':

1. Streamline the acquisition of CDS. It's not a ship, it's not a new kind of tank. Why is it taking so long?

2. DoD, get the policies done! Listen to the tactical environment. Are the policies and processes doable? Are they functional? Need to do things in incremental stages. Use the 'CDS memos' to get guidance out to the field quickly.

3. Cyberspace. UCDMO needs to be the facilitator, the matchmaker.

4. Vendors: 'the cyber threat is eating DoD's lunch'. Bake in security, don't try to bolt it on later. Point to point is not the priority any more. Enterprise is.

5. Funding.

In closing, our 'burning platform' must be addressed:

1. Collapse, consolidate, enterprise.
2. Contingency network planning.
3. Stop the stove pipes.
4. Unburden the war fighter.
5. Use CDS.

‘Use the UCDMO. They are at your beck and call.’

0900 Dr David Bray on ‘Responsible Information Sharing and Safeguarding Across Government Domains’.

Dr Bray specifically focussed on counter-terrorism, national security, and homeland security. The information sharing needs of front line investigators are his primary concern.

In an ideal world, information finds you. You don’t have to search for it. Something like the Amazon.com recommendation system watches what other people are doing, what others are expert in, and what others are collaborating on around you, and tells you, ‘hey, you might want to get in on this’.

‘Targeted information discovery’.

‘National security requires collectively intelligent actions’.

Of course, you must also protect privacy and civil rights, safeguard sources and methods, share across missions and agencies, and share across domains and partners. These are the ‘responsible’ part of information sharing.

What are the authorities? Look at the president’s Information Sharing Environment (ISE) for an example. The following is from Section 1016 (‘Information Sharing’) of the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, as amended. This was revolutionary in 2004. `www.ise.gov`

It has the following attributes (either nine or fourteen depending on how you count):

(A) connects existing systems, where appropriate, provides no single points of failure, and allows users to share information among agencies, between levels of government, and, as appropriate, with the private sector;

(B) ensures direct and continuous online electronic access to information;

(C) facilitates the availability of information in a form and manner that facilitates its use in analysis, investigations and operations;

(D) builds upon existing systems capabilities currently in use across the Government;

(E) employs an information access management approach that controls access to data rather than just systems and networks, without sacrificing security;

(F) facilitates the sharing of information at and across all levels of security;

(G) provides directory services, or the functional equivalent, for locating people and information;

(H) incorporates protections for individuals privacy and civil liberties;

(I) incorporates strong mechanisms to enhance accountability and facilitate oversight, including audits, authentication, and access controls.

Applies to five communities: Law Enforcement, defence, intelligence, homeland security, and diplomacy.

And it needs to scale; it must be decentralised, distributed, coordinated, and interoperable.

Before 9/11, each US government agency purchased its own infrastructure and IT separately. But inter-agency firewalls precluded information sharing amongst agencies, and this was all right last century, because prior threats generally only affected a single agency.

Discussion of standards to accelerate Federated Identity Management for ‘security at the data level, interoperability across the enterprise’. We are going to need tags now for Controlled Unclassified Information (CUI). We need simplified sign-on. Example: a law enforcement login to JNet automatically provides credentials for access to Intellink, and access is controlled at the appropriate level for them. When the JNet login is suspended, the credential to access Intellink goes away automatically.

The 2007 National Strategy for Information Sharing; anchor to 2010 National Security Strategy.

‘The best government standards should become industry standards.’

The DoD CIO mentioned that they have not put out a Cloud computing security strategy yet. Discussion about the government’s response to Wikileaks—that response shut down and hindered a tremendous amount of information sharing. The DoD CIO’s office tells us that the reason for that response was political. They had to show they were doing ‘something’. Quote: ‘It just got so political,’ she said.

Back to Dr Bray: there are two bookends: Federated Identity and Metadata Tagging. What is in the centre of them? Getting information itself to go find users who need it.

The DoD CIO then mentioned Attrubute Based Controlled Access (ABCA) as a potential enabler.

Question from the audience on metadata tagging. There are different types of metadata, from mission data tags, such as where a photo was taken and when, and other types of tags, like security classification tags. What protects information in the presence of those tags (for example: law enforcement access)? Federal law protects it.

Comment from the audience on the IA workforce: there are currently not enough people with experience in military and IC; the universities are only a source of inexperienced Level 1 analysts. Competition due to demand from the commercial world is eating the supply of experienced people up; who can afford to offer salaries comparable to what the commercial world can pay? The DoD CIO hopes that some people will come to work for the government, even at significantly lower salaries, out of a sense of responsibility to the country.

0945 Frank Sinkular on ‘Keeping Pace with Cyber, the UCDMO Perspective’.

‘Where does the UCDMO come from and what does it need to focus on?’

Both CIOs are now definitely behind the idea of getting people to the enterprise. UCDMO is strategic, tactical, and operational. UCDMO is heavily involved in AFPAK. Was that a success? Partially. But they learnt a lot doing it.

DSOC five point cyber plan:

Interesting anecdote: Mr Sinkular described how UCDMO reacted strongly to DoD’s decision to ‘sensor’ (confusing homophone with ‘censor’) their CDS devices after Wikileaks happened. DoD wanted to open all those CDS devices and install sensors on them. UCDMO said, ‘Oh no you don’t! We designed those things not to talk to the outside world. You’re not going to go make them communicate in ways we didn’t certify. You leave them alone!’ And DoD backed down.

Partnerships are important to UCDMO:

1. Reinforce partnerships with DoD and IC.
2. Strengthen partnerships with industry and vendors.
3. Expand partnerships with DHS, State Department, allies, and NATO.
4. Forge partnerships with Federal civilian agencies.

Governance and Oversight:

- UCDMO want to be a trusted SME and honest broker.
- Risk based decisions, strategic planning, and knowledge management.
- Provide recommendations for relevant cross domain policies.

Enterprise:

- Partner and lead cross domain enterprise architecture efforts.
- Promote and enable secure enterprise.
- *UCDMO cannot spend time and scare money on CDSes that won’t ever see the light of day.*

Targets:

1. CD enterprise capabilities.
2. Promulgate CDS guidance.
3. Build mission operations.
4. Expand engineering resources for hands-on support to CDSE engineering.

UCDMO needs to hire some more smart people, he said.

Back to hitting on the CD enterprise strategy. They are working on an enterprise wide transfer portal in DoD. They are working on a portal project for the IC to connect war fighters to Intellink. Promote the CDS devices that are out there for the CDS vendors like Radiant Mercury.

Roadmap for CD enterprise architecture: ‘once we have the metadata right, do we even need cross domain?’

One domino at a time:

- CSTG published 800-53 ‘overlays’ vice ‘profiles’.
- Develop CDS guidance.
- One standard CDS security assessment report format (not DIACAP’s version, FISMA’s different version, etc.)
- Make reciprocity happen.
- Central repository for security reports.

Key Findings from AMN Tactical CDS Employment:

- configuration management of CDS is important.
- improper installation
- remote management and remote maintenance were taboo words until recently.
- training of sysadmins for CDS

UCDMO policy activities:

Baseline memo will be signed soon. UCDMO is mentioned in the new 800-53 and DoD policy when you see the new revs some out.

DoDI 8500.2 revision expected in Q1 of FY 2012.

CJCI 6211.02D expected in Q4 of FY 2011.

ICS 500-XX expected in Q1 of FY 2012. IC standard for operating CDSes in the IC environment.

Summary of Mr Sinkular's talk:

1. Scalable, dynamic, defensible networks.
2. Cyberspace elevated into operational domain.
3. The enterprise must be defensible, because an enterprise portal will automatically attract attackers.

Note: I am following Track 4 of the technical programme.

1115 Cindy Hart, UCDMO on 'DoD SABI Transition and CDIF Update'.

When the CD memo came out recently, it was an important step forward. CDSE memorandum was an action memo. It requested establishment of CDSE, set up resources and funding. They are looking for a signature on the memo in the next few weeks to make it official.

Full acceptance of SABI tasks beginning 30th September 2011. Realistically, it won't be 30th September, it'll be a few months after that. But it won't be a year from now.

CDIF: Cross Domain Implementation Framework—trying to streamline operations and gain efficiencies and reduce duplication.

CDIF mapping to the Risk Management Framework (RMF): CDRB is the Cross Domain Resolution Board. It wants to *fast-track* known solutions from the baseline—where a full CT&E is not required—and slow-track new development.

What will the CDRB be doing?

- It will become a risk mitigation recommender.
- Then kick over to the regular C&A process.
- This is what the Flag Board agreed to.
- CDRB will be an SME in the CD arena, providing recommendations only.

Moving forward:

1. SABI transition: CDSEs provide more oversight.
2. IC partnership: to satisfy both DoD and IC needs; support both DoD's centralised and IC's decentralised processes.
3. Azimuth check: DoD/DNI leadership changes and lessons learnt.
4. CDIF 2.0: framework in process, gaining effectiveness for the operator.

Dennis Ruth of DSAWG (DISA) stood up to discuss peering relationships with DHS and FAA. For example, NOTAM delivery is critical. There are peering relationships with FBI already. Each of these agencies has the equivalent of CDS in their organisation.

Question from the Navy CDMO: the Navy is fee-for-service. It is costing us $20K per ticket, and we expect 200 tickets. Who is going to pay for the fast track? Will there be a type accreditation process for our CDS situation, where we often install very similar systems on very similar decks?

Answer: we got the same question from the Army. Have to get the answer from the Flag Panel.

Comment from the audience: right now, NSA provides (what looks like) free labour. DoD has a huge IT budget; will NSA go to a fee-for-service model? Fee for service might not even be the right model.

Response from CDSE: not trying to get out of it, just find more efficiencies to be able to accomplish the mission with less funding and fewer resources.

Question from the audience: with SABI transition coming to fruition, will this mean an update to 6211-02 C/D ?

Barbara Fleming said: yes. Intend to put it in 8500.01 and 8500.2 also. For those who have seen the draft CDSE memo, it calls out high level responsibilities.

Expect a DoD Instruction on cross domain.

They are trying to get a joint DoD and IC memo signed.

Question from the audience regarding specific use of CDS overseas.

Answer: talk to CENTCOM about 25/200.

Question regarding Mr Nomen's question about the Navy being fee-for-service: is there support for standing up your own CDSE service, just so you can avoid the fees for service?

Answer: the CDSE memo says that components can set up their own CDSEs, but not below that level, specifically so as to preclude proliferation of too many CDSEs below the COCOMs. Currently, only five CDSOs are authorised.

[definition: CDSE = Cross Domain Service Element]

The Navy CDSO is a full voting member of the CDTAB. The language in the policy needs to use the word 'shall' or 'will' in what the COCOMs do with their respective CDSEs.

1400 Kurt Elean, Senior Policy Advisor, in what used to called ASD(NII) and is now called DoD CIO, DASD(IIA).

On the DoD IA policy portfolio managed by this shop (around twenty or so in all).

First, 8500.01 and 8500.2. 8500.01 is the capstone directive, short and sweet. 8500.2 is the implementation; it used to be longer that it is now because it used to contain a catalogue of security controls. Both of these are being updated very soon.

Moving away from DoD security controls to NIST (i.e., Federal) security controls instead.

They want to make reciprocity happen.

Synchronisation with 8510.01, 8530, 852x, etc.

8510.01, DIACAP, will likely no longer be called DIACAP. They are not sure what it will be called because DIARMF is a terrible sounding acronym.

The term 'C&A' is a sunsetted term. The new name for C&A is A&A. This will avoid confusion with 'CNA' meaning Computer Network Attack.

The new 8500 documents will contain new guidance on SCADA and PIT risk management.

Primarily, they are changing only some of the terminology. There will be a transition period after the new 8500.2 is signed. No sharp turns expected.

The DoD transition will be mostly in terminology. DIACAP matches the NIST SP 800-37 Risk Management Framework (RMF) well enough, so the new DIARMF or whatever it's called will transition smoothly.

DoDI 8510.01 (DIACAP) is merely DoD's implementation of NIST SP 800-38, after all.

8500.2 will implement CNSSI 1253 and SP 800-53. Sunsetting of 8500.2 security controls. The controls will be those of 800-53. System categorisation per CNSSI 1253.

The new 8500 series will align with all NIST and CNSS transformation instances.

1415 Roger Caslow, Chief of Risk Management/Information Security Programmes, ICIA. The following information is all under the heading of the Office of the Director of National Intelligence, IC CIO.

Mr Caslow began with a question for the audience: does anyone know why we decided to dump DCID 6/3?

The answer is: it lacked implementation details.

ICD 503 has an implementation focus. Frank Sinkular said he hoped for a CDS policy. Mr Caslow hopes for a DoD policy. They should just call this the 'hope' conference.

Why ICD 503?

It was founded on the C-I-A triad (DCID 6/3 was founded on 'protection').

It supports responsible and secure information sharing.

It has emphasis on balance of risk and trust.

Informed security decisions at all levels. ICD 503 has some appendices, just like DCID 6/3, covering such things as information security architecture (ICS 503-1), security controls (ICS 503-2), risk management (ICS 503-XX), FVEY access (this is a revised DCID 6/3 Appendix E on foreign persons), media markings, and media sanitisation guidance.

In ICD 502, there were five gapped policies that existed in DCID 6/3 but not in ICD 503.

The six phases of RMF application:

1. Categorise; 2. Select security controls; 3. Implement; 4. Assess; 5. Authorise; 6. Monitor.

ICD 503—the transition: NSA and Navy have already begun their transition. NRO began a hard transition June 1. DIA to begin transition this year.

Training on ICD 503 began in May 2011. Two classes are offerred through ODNI, a two day class for senior managers and a five day class for IA professionals. Next course 17–18 August in Chantilly. To sign up for the class, contact Cindy Hart at UCDMO. They are seriously encouraging ANYONE who is interested to take the training. Mr Caslow will smooth the way personally for anyone whose management gives them trouble over taking the training. They really want to train a lot of people on ICD 503 now.

Vendors are welcome and encouraged to take the ICD 503 training.

Bottom line: DCID 6/3 replaced by Summer 2011. They have delivered 4 of 5 core joint task force transformation initiative working group (collaborative IC–DoD–Federal Civil communities) policy documents through NIST. 'We are in the business of information sharing.'

Outcomes: US IC, DoD, and Federal Civil aligned for greatest impact.

Question from the audience: DoD 5200.40 programme protection is missing from ICD 503. How do we get programme protection planning folks involved?

Answer: There is talk of fully integrating what we think of as C&A (now A&A) into the acquisition process. Security controls will become just more contract requirements to be written into the RFP and handled as CDRLs rather than as specially prepared documents. The IA experts are trying to make sure that IA requirements do not become reduced to lip service.

ODNI will be publishing a handbook soon, about the same size as the old DCID 6/3 handbook, for PMs and acquisition folk to read.

Question from the audience about legacy profiles: how to re-use old evidence packages based on Protection Levels and referring to DCID 6/3 security controls?

Answer: lots of people have done mappings from DCID 6/3 to NIST SP 800-53, but they were all different. (This prompted another question from the audience: how are you going to address the moving target problem with Rev 4?)

Answer: ODNI updating the baselines for Rev 4 already. There is no issue here. As soon as Rev 4 is published, they will look at 1253 and update it immediately. For example, if a C&A were in progress under DCID 6/3 today, there is no problem. The C&A will run to completion normally, then under the continous monitoring process, the next time they need to update their security documentation package, they will do it according to ICD 503 and NIST SP 800-53. They are not going to shut down a DCID 6/3 C&A just because.

Categorisation of the system gives you the baseline. Then you apply the appropriate overlay (INT, tactical, whatever). There will be a couple of classified overlays, for formats that we do not want to share with other governments. In cases where overlays conflict, there is already a simple resolution protocol: just leave the security control in (after all, it provides some protection). If one overlay says take it out, and another overlay says leave it in, then leave the security control in.

Question from the audience about reciprocity. What does 'reciprocity' really mean?

Answer: If you bring me your documented evidence package, showing what you tested, how you tested it, and documentation that you did the testing the way you say you did, then I will look at it and see what you have already done. I am not going to re-do tests that you have already done and documented that you did.

Reciprocity does not mean accepting others' *authorisation*, only the documented evidence of tests already done. If the new agency's own risk assessment differs from yours and calls for additional tests, then only those additional tests will be run and must be run.

For example, when CIA passes a body of evidence to PACOM, today PACOM wants to re-run all the tests CIA already did, and that's wrong. That is not how reciprocity is supposed to work. 'It is a waste of money and we are in a budget crunch.'

1545 Kelley Dempsey of NIST, on 'NIST Special Publications'. (She works for Ron Ross.)

NIST SP 800-53 Rev 3 (security controls)

800-37 Rev 1 (risk management framework)

800-53A Rev 1 ('Guide for Assessing the Security Controls in Federal Information Systems and Organisations') ¡– this is NOT the same as 800-53. People get them confused all the time.

800-39 ('Managing IS Risk')

and coming soon, 800-30 Rev 1 ('Guide for Continous Risk Assessment'),

800-53 Rev 4 (fully updated with new sections on Insider Threat, application security, Supply Chain Security, advanced persistent threat, SCADA, mobile devices, Cloud Computing, and privacy controls). SP 800-53 is on a two year revision cycle; it seems like they just changed this but it's really on schedule to be updated this year.

800-128 ('Security Focussed Configuration Management')

800-137 ('Continuous Monitoring Guideline')

Later on, there will come a Systems and Security Engineering Guideline, but it doesn't have a publication number yet.

NIST reads all public comments and considers them carefully. SP 800-53 Appendix J ('Catalogue of Privacy Controls') is out for public comment now.

Next, the presenter went into some conventional and unconventional threats to security:

1. Conventional threats to security: description of the Stuxnet worm, flash drive incident in DoD, stolen laptop incident in the Department of Veterans Affairs. These last two incidents prompted real changes: in the first case, causing DoD to ban all use of flash drives, and in the second case, a long-overdue

enforcement of full disk encryption on all US government laptops. A later security incident of another lost laptop shortly after the VA stolen laptop incident was a non-incident as a result of the change in practice.

2. Advanced Persistent Threat. The key word is ‘persistent’. An adversary with high levels of expertise and resources, who uses multiple attack vectors and hides effectively, because they want to be in your system for a long time, undiscovered, so they can exfiltrate large amounts of data. The APT adversary characteristically has both *capability* and *intent*.

3. Unconventional threats: connectivity and complexity.

The evolution of risk and security: at first, we focussed only on confidentiality protection; now, we pay more attention in addition to integrity and availability too. Before, risk and security were considered at a static point in time; now, it is continuous. Before, we thought of government-only systems; now, we think of commercial products. Before, it was all about risk avoidance. Now, we think in terms of risk management.

Inhibitors to cyber security success: bureaucracy, inability to innovate, lack of flexibility in building useful security solutions, culture and institutional barriers, poor intra-agency communications, lack of senior leadership committment, fear of auditors, and no true risk management.

NIST SP 800-39 introduced a multi-tiered risk management approach, implemented by the Risk Executive Function, as well as an enterprise architecture and SDLC focus. The three tiers of the risk management approach are:

1. organisation, i.e., governance; this is the realm of 800-39.
2. mission/business process, i.e., information and information flows;
3. information system, i.e., the environment of operation; this is the realm of 800-37.

Risk Management in 800-39 seeks to broaden the narrow view that Information Security is only a technical matter or a stove pipe independent of organisational risk.

Key elements for effective risk management: it must be focussed on the senior leadership. *Assignment of responsibility to senior leadership* is very important.

The Risk Executive Function (REF) is a functional role that provides a comprehensive organisation-wide approach to risk management. The REF coordinates with other senior leaders to establish risk management roles and responsibilities.

Components of Risk Management:

I. Framing risk
II. Assessing risk
III. Responding to risk
IV. Monitoring risk

NIST SP 800-37 Rev 1 shifts the focus to holistic RMF process. It integrates RMF into the Software Development Life Cycle. It provides tasks for each of the six phases in the RMF:

1. Categorise (FIPS 199 and NIST SP 800-60 are applicable)
2. Select (FIPS 200, 800-53 applicable)
3. Implement (many of the 800 series SPs are applicable here, for example the 800-70 checklist)
4. Assess (use SP 800-53A and 800-115)
5. Authorise (here is where the POA&M comes into being, the authorisation package, and OMB circular A-130 for Federal civilian systems)
6. Monitor (use 800-137 DRAFT).

Moving right along into 800-137 DRAFT, we have the idea of Continuous Monitoring, with the following activities in the strategy:

- define
- establish
- implement
- analyse/report
- respond
- review and update

in a cycle, of course.

NIST SP 800-128 is expected to be published this week. It covers ‘Security Focussed Configuration Management of Information Systems’. It has four phases:

1. planning, where you develop a CM plan, establish a CCB, and develop an IS component inventory;
2. Identifying and implementing a configuration;
3. Controlling configuration changes phase;

4. Monitoring phase.

Question from the audience: is there an equivalent to the Risk Decision Acceptance Criteria (RDAC) in these SPs somewhere?

Answer: yes, some of it is in 800-39 and more of it in 800-30. You haven't seen it yet because 800-30 hasn't been relased.

Question from the audience: where is guidance on the proper intervals to choose for periodic events?

Answer: there are no specific numbers in the SPs because every system is different. Use the guidance to choose reasonable and applicable frequencies for your organisation and application.

Question from Karen Burke of NPS: will FIPS 199 and FIPS 200 be updated?

Answer: probably not.

Question from the audience: credit card companies have PCI requirements calling for seriously aggressive penetration testing—not just nmap scans but seriously attempting to break in—and some brokerage houses are doing this monthly now, with POA&Ms at 30 day intervals. Is there any thought given to including a requirement for ongoing penetration testing in the continuous monitoring phase?

Answer: NIST will take that back as a public comment and see where it fits in.

References