Virtual "Coffee Chat": NIST SP 800-171 and CUI with Ron Ross

Presented by the EDUCAUSE Cybersecurity Initiative
September 29, 2016

Chat Transcript

Karen A. Wetzel, EDUCAUSE: Welcome, everyone! Today's EDUCAUSE InfoSec virtual coffee chat on NIST SP 800-171 with Ron Ross will begin at 1 pm Eastern Time. Chat with attendees using this chat area or tweet using this hashtag: #HEISC

Karen A. Wetzel, EDUCAUSE: Again welcome! Feel free to weigh in on our first poll question -- at the bottom right of your screens.

Karen A. Wetzel, EDUCAUSE: We'll be starting in just a few minutes. Feel free to introduce yourself in this chat area!

Amanda Sarratore: Hello everyone! I am with the University of Notre Dame and I am looking forward to getting more information on this topic.

Matthew Nappi: Hello All. I'm the interim CISO at Stony Brook University. This has been a hot topic of discussion lately. I'm looking forward to the session.

Sharon Pitt: Hi fellow SUNY colleague. :)

Brian Martinez: Brian Martinez, Michigan State University. Presently with the Internal Audit Department.

Matthew Nappi: Hi Sharon! Nice to "see" you!

Jason Stein - Purdue University: Hello, all. I'm an IT Security Analyst at Purdue University, and recently published a paper on this topic with EDUCAUSE about our solution. I'm looking forward to seeing what others are doing.

Melissa Woo - Stony Brook University: Hi all, I'm the CIO at Stony Brook

University, and I'm really not spying on Matthew... honest! :-)

Melissa Woo - Stony Brook University:*waves at Sharon*

Sharon Pitt: Hello Melissa!

ScottF - UAB: Good morning and afternoon everyone. Good to see all of you.

Matthew Nappi: Ha! Don't believe her. Hi Melissa!

M'Shiela Hawthorne: Hi everyone. M'Shiela Hawthorne from North Carolina State University Internal Audit.

Ben Woelk (Rochester Institute of Technology): Ben Woelk, Program Manager in the Information Security Office at the Rochester Institute of Technology. Member of HEISC A&T working group.

Karen A. Wetzel, EDUCAUSE: If anyone has technical difficulties today, please send me a note in this chat.

Michael Corn (Brandeis University): Hi all!

Todd H: looks like it's being recorded. correct?

Melissa Woo - Stony Brook University: *waves at Mike Corn*

Mike Chapple (Notre Dame): Hello, everyone!

Christina Bonds - Elon University: What is the phone number to dial in?

Melissa Woo - Stony Brook University: *waves at Mike Chapple*

Dewight F. Kramer: Hello Everyone (UC Davis)

Tracy: Ciao!

Karen A. Wetzel, EDUCAUSE: In addition, use this chat space to chat with attendees or ask the speaker questions. You can tweet about this event using the hashtag: #HEISC

Jason Pufahl: Mike Corn!

Melissa Woo - Stony Brook University: Jason Pufahl!

Michael Corn (Brandeis University):Hi Jason!

Karen A. Wetzel, EDUCAUSE: We are recording this event. The audio recording, slides, and transcript will be available shortly on the EDUCAUSE Cybersecurity Initiative website: http://www.educause.edu/security

Jake Cunningham - UMASS Amherst: Hi Jason!

Valerie Vogel, EDUCAUSE: It's great to have such a big crowd for our first virtual coffee chat! :)

Dan Wood: Good Afternoon Everyone!

Jake Cunningham - UMASS Amherst: Hi Michael!

Josh Dunbar: ISSA at Virginia Tech

Jason Pufahl: Hi Melissa :)

Melissa Woo - Stony Brook University: Good to see so many people I know here.

Michael Corn (Brandeis University): It's like a reunion going on here.

Andy Weisskopf (Binghamton): Everyone! :)

Melissa Woo - Stony Brook University: And Andy too! Hi Andy!

Robert Renaud: Looking forward to learning more!

ScottF - UAB: Agreed Melissa! Missed all of you that I usually see at SPC. hopefully next year I will get to go.

Valerie Vogel, EDUCAUSE: For Ron's complete bio, please see: http://csrc.nist.gov/staff/rolodex/ross_ron.html

Patrick Feehan - Montgomery College: Hello All

Neal Fisch/CSU Channel Islands: Hi to all EDUCUASE buds!

Melissa Woo - Stony Brook University: ... and Patrick ... and Neal! Hi!

Patrick Feehan - Montgomery College: Melissa - Stony Brook!!

Brad Judy: Greetings

Melissa Woo - Stony Brook University: Hey, you need to keep up, Patrick. ;-)

Patrick Feehan - Montgomery College: I actually knew - followed you since Milwaukee days. Congrats

Melissa Woo - Stony Brook University: Thx Patrick! Hope all is well with you.

Jane Rosenthal (Mines): audio is spotty

Josh Dunbar: Audio is good via phone

Matthew Nappi: Audio sounds fine for me via the Adobe connect room.

Brad Judy: Audio good via computer here

Kyle Johnson (Chaminade Univ): Audio is good for me to via Connect

Sharon Pitt: Audio is fine for me with Adobe Connect

Becky Fowler: not working in adobe connect room for me

Neal Fisch/CSU Channel Islands: Adobe audio is fine for me as well

M'Shiela Hawthorne: Are there links to the PowerPoint presentation?

Jane Rosenthal (Mines): better now

Karen A. Wetzel, EDUCAUSE: We will be providing the slides as well as a link to the recording of this webinar will be made available on the EDUCAUSE Cybersecurity Initiative website at http://www.educause.edu/security

Larry Knotts: https://educause.acms.com/ecar/ This will link you to presentation

Karen A. Wetzel, EDUCAUSE: If you are having trouble with audio in the Adobe Room, feel free to dial in with your phone. Access information is available at the bottom right of your screen.

M'Shiela Hawthorne: Thank you

Karen A. Wetzel, EDUCAUSE: Don't forget to add your questions in this chat area throughout today's event! You can also tweet your thoughts using the hashtag #HEISC

Valerie Vogel, EDUCAUSE: CUI Registry: www.archives.gov/cui/registry/category-list.html

Brad Judy: I think a lot of folks here will be interested in some discussion on the DoEd dear colleague letter that references 800-171 as a standard for student data - that has major implications.

Isaac Straley - UCI: I'm particularly interested if: 1) 800-171 will be a requirement for FERPA data from Department of Ed/Financial Aid data and funds and 2) Will there be a new assessment and compliance reporting process?

Dewight F. Kramer: Isaac!

Kyle Johnson (Chaminade Univ): Ditto @brad and @iMac

Isaac Straley - UCI: Dewight!!

Mike Chapple (Notre Dame): Yes, agree. Some insight on DoE plans would be very helpful.

Kyle Johnson (Chaminade Univ): sorry @Isaac

Larry Knotts: Karen: I'm in charge of FISMA compliance for Emory University research endeavors mostly funded by DHHS and subordinate agencies. Currently, all the contracts are specifying IT-SC&A according to NIST SP 800-53, when may we expect to see reference to NIST SP800-171? Who should we expect to instigate the change in the contract language? Thanks.

Brad Judy: The wording of the DCL wasn't that it was "required" but referenced it as a standard they might reference in an audit, so an implied requirement?

Melissa Woo - Stony Brook University: We would also be interested in the implications of the Dear Colleague letter.

Antonio Crespo (Barnard College): Hello everyone.

Kyle Johnson (Chaminade Univ): Anybody know who the dear colleague letter went to? I've heard nothing from any of our functional offices about this

Brad Judy: Hi Larry - I used to work for Brad Sanford at Emory

Dave 2: Effective Dec 2017, non-federal entities are required to comply with 800-171; are federal entities subject to the same compliance deadline?

Andy Weisskopf (Binghamton): Kyle, financial aid

Brad Judy: Kyle - typically the student functional folks get it - registrar, etc.

Larry Knotts: Hi B. Judy

Dewight F. Kramer: Along with @brad and @Isaac , we are curious how research will need to comply with NIST 800-171

Brad Judy: https://ifap.ed.gov/dpcletters/GEN1612.html

Brad Judy: for those who haven't seen the DCL

Antonio Crespo (Barnard College): The DCL ambiguity has our General Counsel and others interpreting it as enforcement criteria and asking us to comply as though it was required…

Jason Stein - Purdue University: Will the upcoming FAR clause for non-feds, referencing 800-171, require implementation of all 100+ elements of 800-171 for all data in the CUI Registry?

Melissa Woo - Stony Brook University: Second what @Dewight said re: implications for research

Karen A. Wetzel, EDUCAUSE: Thanks all for the questions -- I'm gathering these so that Ron can answer them at a break.

Jane Drews: I believe all federal funded research will eventually have to comply.

Jane Drews: federal agencies have 800-53 to meet

Tim Tolson from University of Virginia: Joining @Dewight @brad & @Isaac in interest in applicability of NIST SP800-171 to research - both grants and contracts

Isaac Straley - UCI: We've already been ramping up a program to meet 800-171 for research, but the FERPA classification was a surprise

Tom Siu - CWRU: @Jane Drews- that depends on the contracting group of the sponsored agency.

Jane Drews: which is what has been used outside of federal because there wasn't anything else to point to.

Brad Judy: FYI - for Federal agencies, student data is listed in the CUI registry, so technically the DoEd has to meet 800-171 for student data themselves, thus why they probably use it in the DCL

Larry Knotts: The 800-171 seems more pertinent to university research systems versus the more comprehensive 800-53. Not that 800-53 will go away for "deep dive" requirements, but the tone and tenor (recognition of non-Fed entity) seems more applicable.

Tom Siu - CWRU: @Brad Judy: DoEd has to meet 800-53, for Federal Data Systems...

timothy spiker: @ Jane Drews - the level of complexity for the 800-53 is reduced with the 800-171

Isaac Straley - UCI: This presentation implies the 800-171 requirement will impact data connected to Financial Aid funds: http://fsaconferences.ed.gov/conferences/library/2016/NASFAA/2016NASFAACybersecurityRequirementsforIHEs.pdf

David Cassada: Just be glad that we aren't required to comply with FISMA ;)

Melissa Woo - Stony Brook University: Yet @David

Valerie Vogel, EDUCAUSE: We hope to answer all of your questions during the Q&A when Ron is done speaking. We will also share his e-mail address in case you need to follow-up with specific questions about NIST 800-171 for your institution.

Dewight F. Kramer: with the deperimeterization of a University network

means that we often do not have defined boarders. We ran into this with PCI and it was a challenge to make sure there were clear boarders for those few networks

Jason Stein - Purdue University: To other University people: Are you absorbing these costs internally, or reflecting them in your contracts with 800-171 requirements?

Josh Dunbar: @Jason absorbing them internally

Dewight F. Kramer: As such, I am a little skeptical when he says, that it is just protect the network or section of the network that has CUI

Jane Drews: absolutely my position tis this is a good thing. previously we had to meet 800-53 for some research, but I've seen at least six recently that now require 800-171.

Jarret Cummings2: EDUCAUSE Policy has started a dialogue with Federal Student Aid about its thinking around 800-171. More to follow as that conversation takes shape.

Matthew Dalton (UMass): FAIR

Mike Chapple (Notre Dame): We are building shared services with central funding and then requiring individual projects to fund their own project-specific needs. Building the entire environment in the cloud.

Brad Judy: Jarret - good to know - we look forward to hearing more

Jane Drews: note that 800-171 is basically a subset of 800-53.

Jason Stein - Purdue University: Mike - Yes, I know. I'm working with Bob Winding. We' meet regularly.

Dewight F. Kramer: We use a mix of ISO, NIST, ITIL

Larry Knotts: We're attempting to get our system owners to consider

potential security costs in their bid, however, it's difficult to estimate and it runs the risk of making the bid non-competitive. I'm hoping to see what Jane Drew alludes to, which is language in the contracts specifying 800-171 versus 800-53. That will be an easier presentation to system owners.

Jason Stein - Purdue University: ND and Purdue share a lot of common ideas related to 800-171.

timothy spiker: @Jarret Cummings2 - please include me in the dialogue

Tom Siu - CWRU: @Jason Stein: 1) for research with FISMA requirements, we make sure the contract funds controls we don't already have, 2) 800-171 is self-funded in mapping our current SANS 20 controls to them.

Mike Chapple (Notre Dame): Yes, I remember meeting you.. Just sharing for everyone else's benefit :)

Jason Stein - Purdue University: I thought I remembered your name.

Jon Cutler: No formal framework, but aligned to SANS/CISC Critical Security Controls

Jamie Lam: (UCSF here) Hi Isaac, Hi Dewight!

Jarret Cummings2: @Timothy Spiker: Please share your contact info with me when you can. (jcummings@educause.edu)

Kolin Hodgson - Notre Dame: Will interpretations of 800-171 requirements would be the same as interpretations of current FISMA Moderate?

Isaac Straley - UCI: Hey, Jamie!

Dewight F. Kramer: Jamie!

Melissa Woo - Stony Brook University: Good to hear that compensating controls can be appropriate

Dewight F. Kramer: The assumption two, is very complex at, at least our, university

Josh Dunbar: How far reaching is 171 in a network environment? Where do you stop protecting it at the 171 level? I've been told it's once you've hit the last authentication mechanism for the systems containing CUI.

Valerie Vogel, EDUCAUSE: FedRAMP: https://www.fedramp.gov/

Tom Siu - CWRU: @Josh Dunbar: Scope management is key, or else the risk picture for a university will be problematic.

Josh Dunbar: @Tom wouldn't that be different for each contract/program that requires 171 compliance?

Jason Stein - Purdue University: @Josh - Purdue decided it was all the way to the endpoint.

Isaac Straley - UCI: Network segmentation becomes a key control, whether this applies "just to research" or more broadly because of new FERPA/etc. rules.

Jason Stein - Purdue University: But we've seen differing opinions in that area.

Dewight F. Kramer: Actually we are just starting to look at AWS for NIST 800-171 environments, and they have a great responsibility control matrix http://docs.aws.amazon.com/quickstart/latest/accelerator-nist/welcome.html

Josh Dunbar: Thanks Jason. I'm part of the team at Virginia Tech that's addressing 171.

K Finley: FEDRAMP is a beast. Hope they are not requiring that. We use the CSA STAR

jeff murphy UB: also, 800-171 calls out mobile computing and limiting its

impact, which implies EMM or something similar, which can get complicated as that's not something we've really explored.

Jason Stein - Purdue University: By request, this is an outline Purdue's 800-171 solution.

Jason Stein - Purdue University: http://er.educause.edu/articles/2016/9/leveraging-cloud-services-for-nist-sp-800-171

Jamie Lam: thanks Jason

Dewight F. Kramer: Thanks Jason

Thomas Trappler: New FedRAMP Accelerated program may help tame the FedRAMP beast? https://content.govdelivery.com/accounts/USGSA/bulletins/167d429

Valerie Vogel, EDUCAUSE: FIPS 200: http://csrc.nist.gov/publications/PubsFIPS.html

Valerie Vogel, EDUCAUSE: Find NIST 800-53 and 800-171 here: http://csrc.nist.gov/publications/PubsSPs.html

Josh Dunbar: If someone is leveraging the cloud, who is responsible for verifying the cloud provider's compliance to 171?

Kolin Hodgson - Notre Dame: https://gcn.com/articles/2016/06/24/fedramp-high.aspx

Tom Siu - CWRU: @Josh Dunbar- note the "inventory" requirements- if your scope is correctly, that can be done, but if your scope if for your full university and all the subunits, that alone could take up years of resources.

Dewight F. Kramer: We use 27001/2

Dewight F. Kramer: @Josh Dunbar, I don't understand your question. We

are looking at the cloud for developing an area for 171

Jason Stein - Purdue University: @Josh - Services that are compliant will call it out and back it up somehow. But be aware: The CSP is only responsible for their portion. Things you build within the Cloud are your responsibility to meet 800-171.

Jason Stein - Purdue University: Purdue uses AWS GovCloud. They call out compliance all the way up to FedRAMP

Jason Stein - Purdue University: And back it up with an ATO

Josh Dunbar: Got it. Thank you, Jason

Fran: How do we get the slides?

Jane Drews: we are already seeing 800-171!!!

Isaac Straley - UCI: *contract* or *contract or GRANT*

Kyle Johnson (Chaminade Univ): I'd suggest EDUCAUSE take all the questions, ask Ron or someone to answer them, and put them on the EDUCAUSE web site as a FAQ. It doesn't make sense to me for everyone one of us to send NIST the same questions over and over

Karen A. Wetzel, EDUCAUSE: We'll be posting the slides as well as a link to the event recording online at http://www.educause.edu/security

Josh Dunbar: +1 @Kyle

Karen A. Wetzel, EDUCAUSE: Kyle -- I'll work with Valerie to do that. We've been sorting your questions throughout today and shouldn't be an issue to get this done .

Kathy Gates 2: thanks, Karen!

Kyle Johnson (Chaminade Univ): Thanks Karen

Karen A. Wetzel, EDUCAUSE: But keep sending them along so we don't miss any! :)

Kyle Johnson (Chaminade Univ): @Karen, could you please include any questions that were submitted ahead of time (I submitted a few)? Thanks.

Karen A. Wetzel, EDUCAUSE: Indeed, Kyle. Will do.

Caroline Miner: Do these requirements apply to information created by the university using federal grant dollars?

Jane Drews: hello financial aid!

Test: Question for Ron: What is the expected evidence of compliance?

Tim Tolson from University of Virginia: He said make sure federal agency is specific about what requirements, but we've seen so far in contracts is the federal agency including an appendix that basically says comply with NIST SP 800-171. Are there documents we can reference to get them to be more specific and tailored to data.

Rebecca Hartley: This week, we received our first subcontract with an 800-171 requirement for data protection (that was not under DFARS, and thus did not have the December 2017 extension). And I second Tim's point. The contracting officers also seem confused about what is required.

Josh Dunbar: VoIP: 3.13.14

U-M AL: For unclassified information - how should we determine if FISMA requirements apply or if 800-171 applies? Is this still based on what individual government agencies state?

sanjay: This is a very specific question: We use Google Apps for Mail/Drive. Can I assume that CUI should not be sent or stored on that platform?

Tim Tolson from University of Virginia: @U-M AL We have some question

Leo Howell, NC State University: Can we expect that the federal government will audit us?

Joanne Kyriacopoulos: Are contracting officers equipped to make that assessment?

K Finley: If a university has a data network in-house (not in cloud) used by the FedGov does it have to be FedRAMP compliant?

Josh Dunbar: Has control 3.8.4 been defined yet? Marking CUI

Josh Dunbar: I'm having folks refer back to 32 CFR 2002 for now

Dewight F. Kramer: yes please

U-M AL: Is there any update on when 800-53 rev 5 is expected?

timothy spiker: yes it would

Capella University - mwalstrom: Yes please to 800-171 alpha

Tim Tolson from University of Virginia: YES! Enthusiastic support for SP 800-171 Alpha document

Jason Stein - Purdue University: Agreed on 800-171 Alpha

Jane Drews: a broader question.... will we have to use 'gov cloud' options for CUI federal data once the FAR is in place?

Karen Monkhouse: yes, want the 800-171 alpha!

Josh Dunbar: Does anyone know if this chat is exportable?

Tom Siu - CWRU: We see HHS's Office of Civil Rights doing the HIPAA audits, so this is what comes to mind about 800-171 applications.

K Finley: is a copy of this presentation going to made available on the EDUCAUSE or ECAR website?

Karen A. Wetzel, EDUCAUSE: Yes, the recording and slides will be made available on our site at: http://www.educause.edu/security

Valerie Vogel, EDUCAUSE: We can also make the chat transcript available!

Dewight F. Kramer: thank you!

Josh Dunbar: Thanks Valerie

Josh Dunbar: That would be helpful

Karen Monkhouse: great, would like the chat transcript also

Denise Dolezal UC Santa Cruz: Please also include recommended reading list as well

K Finley: Does ITAR data require FedRAMP High Accreditation?

Karen A. Wetzel, EDUCAUSE: Absolutely, Denise. We'll do that.

Tim Tolson from University of Virginia: Having slides, recording, and chat transcript available is great. Thank you very much!

Karen A. Wetzel, EDUCAUSE: If you haven't yet filled out the evaluation form, please do so! Thanks everyone for joining us today.

Tom Siu - CWRU: Thanks Val!

Melissa Woo - Stony Brook University: Thank you - very informative!

Dave - Oregon State University: Thanks!

sanjay: Thank you

Josh Dunbar: Thanks everyone.

Jane Drews: thanks to Ron, this has been very useful information.

Cheryl Welsch: Thank you!

Jamie Lam: +1 on recommended reading list

Jamie Lam: thank you!

Wendy Epley: Thank you, Dr. Ross, Karen, and all for your guidance.

M'Shiela Hawthorne: Thank you!

timothy spiker: thanks all

Kathy Gates 2: this was a great topic. I hope we have more sessions to continue to help us figure this out.

Dave 3: Very good! Thank you

Tim Tolson from University of Virginia: Thank you - great topic, informative and helpful presentation. Thanks to Ron Ross.

Bing Li (University of Nevada Reno): this was a great presentation. I learned a lot. thanks

Jane Rosenthal (Mines): this was an excellent talk--

Valerie Vogel, EDUCAUSE: Thanks so much for your participation today!

Jane Rosenthal (Mines): what Kyle said about making FAQs would be awesome