

File 20091023.0533: Weekly activity report 0107:

weekly activity report 107 (loughry)

Joe Loughry

Sent: 23 October 2009 05:33

To: andrew_martin_comlab_ox_ac_uk; Niki Trigoni; Joanna Ashbourn

Cc: andrea@hpwtdogmom.org; Joe Loughry

Attachments:

Weekly activity report no. 20091022.2111 (GMT-7) sequence no. 0107, week 2 MT

I met with Dr Martin on Monday by video teleconference. I described the U.S. Air Force proposal that I had worked on all week. It was mailed on Friday last. The proposal is for one year's funding to build a certification and accreditation (C&A) tool specific to AFI 33-210, a tailored DIACAP. The call for proposals requested a single-purpose tool, but after considering it I decided to submit a proposal for a somewhat more general tool that would be applicable to more organisations than just the one requesting proposals. It is a risk to propose a solution different from what the requesters asked for, but I think that in this case the risk is worth taking. If I get funding, it will be for this year. As of today, the requester has acknowledged receipt of all proposals but nothing more. I know that someone there noticed my proposal, though, because they commented in their acknowledgement on the name I gave to the tool: nihil obstat. (It seemed like a good name for a C&A tool.)

Right before sending in the proposal, an opportunity arose to get access to the entire Certification Test & Evaluation (CT&E) data for a major software update to an existing computer system under NIST Special Publication 800-53---a good validation test case for a general C&A tool. I wrote that into the proposal at the last minute. I have an invitation and approval from the owners of that system, who are starting CT&E soon, but I have not got access to the data as of yet. 800-53 is brand new (August 2009) and even the Certification Authorities are not familiar with it yet. The need for a C&A tool is even more acute.

I promised to send a draft of the Crosstalk article to Dr Martin by tomorrow; I am working on it now. Trying not to drift, as Dr Martin cautioned against.

This week I volunteered to introduce the next paper at Reading Group; I chose a recent article on getting support for risk management by information security practitioners in industry. I can validate some of what the authors claim in the paper with my own experience in the banking and defence contracting industries, and I want to compare the different attitudes towards risk avoidance vs risk management in DoD and MoD.

Deadlines and Tasks this week: I owe the Air Force a summary progress report tomorrow. I owe Dr Martin a draft of the Crosstalk paper tomorrow.

Next meeting planned for: Wednesday, 28th October after Reading Group.

Joe Loughry

Doctoral student in the Computing Laboratory

St Cross College, Oxford

End of WAR 0107.

References