From: Patel, Swati
To: Soura, ChristianChristianSoura@gov.sc.gov
Date: 10/25/2012 8:56:26 AM
Subject: Re: 2012-xx Appointing a statewide IT security advisor

Great thoughts. I will work with this.

From: Soura, Christian
Sent: Wednesday, October 24, 2012 11:50 PM
To: Patel, Swati
Subject: RE: 2012-xx Appointing a statewide IT security advisor

I've read it a couple of times, and I'm still brushing up against the same issues I had earlier. Without rehashing all that, it seems there are a few questions that we have to answer in some way, whether explicitly in the document, or else at least in our heads as a vision for this thing is more clearly formulated:

1. Who will this person report to? If the EO is silent, then presumably the Governor?
2. What is the work product? Is a report due…and if so, when, and to whom? Are there meetings of some kind? Is there a workgroup to be created?
3. What's the scope of this work? It is just cyber-security, narrowly defined to technical issues? If it's "information security" more broadly, then this creeps even further into the IG's domain. The 2nd "whereas" strikes me as being associated with a much broader mandate than the other items suggest.
4. For what period will this person do this work? Does this position effectively sunset at some point, whether that be a date certain, or upon some trigger event, like the submission of a report?
5. How will this person interact with all the other people, policies, and programs that already exist in this space?

I don't have and/or haven't heard very good answers to most of these questions at this point, and so I don't really have proposed edits/language, either. To briefly address them, though…

1. I don't know how this person could report to anyone other than the Governor. A Chief Information Security Officer would typically be subordinate to a state's CIO, and I understand there's a roughly comparable position here already (although without a strong central IT function, his job is fairly different than a CISO's job would be in a state with a more coordinated approach to technology). A (presumably) limited-term advisor like this probably has to report to the Governor, since that's who's creating this thing.
2. The EO already speaks to recommendations, which screams "report" to me. So I think we might as well be explicit in that regard. If this person reports to the Governor, then the report might as well be due to her, although the EO could also say that the report would be provided to others, such as the IG, Marcia and/or Jimmy, and even the presiding officers maybe. I'd be reluctant to create additional committees to go along with this.
3. You can go several different ways with this. A narrower mandate gets you a faster report, if that's important. I don't know what kind of resources would be committed to this, but if it's basically a guy with a clipboard (the vibe I'm getting), then you might focus on getting specific recommendations for policy changes…those would arise from this person's interviews/walking around, but would also have to arise from his/her direct expertise in this field and knowledge of best practices. For instance, we should be locking down USB ports on our computers to help (1) keep data from walking away, but also (2) folks from bringing viruses onto our network. This is a recommendation that basically anyone could make for us. That said, if it's "a guy with a clipboard," then I'm not sure that broader, strategic recommendations would be widely perceived as valid. What I mean is that anyone who has experience in this field would look at the status quo here and tell us we're crazy for failing to address IT security as an enterprise…which means that if you invite strategic/vision recommendations, then they're basically going to make a DOA argument. Although that's entirely reasonable and appropriate, it would give what are not intended to be "political" recommendations an apparent political flavor. In the middle, at the operational level (between day-to-day policies and the strategy/vision), there are significant decisions to be made about the equipment the state owns or leases…what do we need to buy (products and/or services)…how much would it cost, etc.? One person won't have the resources to

effectively consider or answer those questions. And if you got answers, you probably wouldn't like them…they tell us to buy $6 million in SiteMinder licenses, for instance.

4. You can't have a report without a due date. I don't know who we think will do this, or who will help them, or how intensive the report would be, etc. Tough to attach a due date, given those circumstances, but I'm guessing this is a 3-4 month thing?
5. This is the hardest question to answer. Part of the reason this should probably be for a limited term with a defined mandate/deliverables is because this is a review of what a lot of folks are already responsible for in some way. This action may be perceived as rather threatening to a number of folks, which makes it all the more important to structure this in a way that's as productive and non-threatening as possible. Maybe this means including language with a more collaborative flavor – gathering input and recommendations from agency staff, think tanks, experts, IT practitioners, etc.

As a final thought, I wonder if we should address training more explicitly…is that something this person should review and offer comments/recommendations on? We already have a series of cyber-security policies (see http://sc-isac.sc.gov) , so you could explicitly reference those and ask this person to proposed specific changes to those, if that's something we want to accomplish. I point this out because the most effective security policies are multi-faceted…they are technological and behavioral. So firewalls and monitoring and retinal scanners are important, but so is telling people to report certain events…or having them change their passwords on a frequent basis. Training (and refreshers) help you address that behavioral component of risk.

Do we currently have agency ISOs? You could conceivably direct agencies to designate those, if we don't…although you'd have to clarify their roles and responsibilities. That might be more of a potential recommendation to come from this new person.

Just so you know…I have numerous agency budget meetings tomorrow, plus a time-sensitive one for the ACT/WorkKeys initiative, so it's gonna be hard for me to put any real time into this tomorrow. I'm open for a few minutes at 9:30, and then it opens up a bit again after 3. Other than that, I'm either locked in the conference room, or else over meeting with the ACT/DEW folks.

CLS

Christian L. Soura
Deputy Chief of Staff

(803) 543-0792
ChristianSoura@gov.sc.gov

From: Patel, Swati
Sent: Wednesday, October 24, 2012 5:05 PM
To: Soura, Christian
Subject: 2012-xx Appointing a statewide IT security advisor

Sorry. Use this one.