From: Tom Watson
To: Brian Mechler
Cc: Charles Pinney; [redacted]; French, Lesley; Cheryl Sneeringer; austin.kinghorn@oag.texas.gov; Christina Adkins
Subject: Re: Vendor Responses to Examiner Questions - EVS 6030 and 6110
Date: Friday, September 4, 2020 1:58:47 PM

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open att
you are expecting the email and know that the content is safe. If you believe this to be a malicious or
please send this email as an attachment to informationsecurity@sos.texas.gov.

Agreed. We should always consider the insider threat.

Tom

On Fri, Sep 4, 2020 at 1:47 PM Brian Mechler <[redacted]> wrote:

> I think it's potentially worse than that. It's a gift wrapped opportunity to an insider threat, however unlikely. I harp on the hash verification process because an insider with sufficient knowledge and physical access can do bad things to systems. How do we thwart that? Through good procedures, one of which is checking that what is installed on the system matches exactly with what was certified by the EAC. Under the current guidance from ES&S, an insider now knows specifically which file is not being inspected. It's similar to a bank robber knowing that the camera covering teller #3 is broken.
>
> It sounds like this was also an issue with the stick upgrade process for 6.0.2.0. Was the SoS ever notified?
>
> Brian
>
> On Fri, Sep 4, 2020 at 12:35 PM Tom Watson <[redacted]> wrote:
>
>> Chuck,
>>
>> I agree with Brian. If the customer is instructed that there is a discrepancy in a hash, they might be inclined to ignore any mis-match. Not sure what the easiest remedy is. We don't want jurisdictions ignoring the hash checks for this release or future releases.
>>
>> Tom
>>
>> On Thu, Sep 3, 2020 at 6:08 PM Brian Mechler [redacted]> wrote:
>>
>>> Chuck,
>>>
>>> The response from ES&S is troubling. There is no paper trail documenting the exception the VSTL made for this breakdown in the hash verification process nor was written documentation provided to or prepared for customers. We are being asked to take ES&S at their word that the VSTL said "this is fine." We are also being asked to take ES&S at their word that they provided appropriate guidance to their customers. This issue apparently also exists for 6.0.2.0, yet it does not appear in any of the examiners' reports. Either this issue was not disclosed or exposed during that exam or there is some nuance that I fail to understand.
>>>
>>> Susan finishes her response by claiming, "Any other modification to that file would also produce a mis-match and be flagged by the export process, providing the information needed to verify the file and detect an external attack." But that is not true. There is already a mis-match and if customers are being told to ignore it, there is nothing to be flagged.
>>>
>>> Can the State of Texas mandate that all upgrades be performed using the full iono install method?
>>>
>>> Brian
>>>
>>> On Thu, Sep 3, 2020 at 9:09 AM Charles Pinney <CPinney@sos.texas.gov> wrote:
>>>
>>>> Brian,