DIAMOND HANDS HOLDING INC.

TO: Jake Bulim, Evan Battaglia, John Smith, Steve Smith, Katie Tylerr

FROM: Ethan Byrd, Cybersecurity Compliance Consultants

SUBJECT: Applying Up-to-Date Information Security Strategies Using NIST

DATE: October 20, 2025

Dear Executives and Stakeholders,

My name is Ethan Byrd, the Cybersecurity Compliance Consultant at Diamond Hands Holding Inc. (DHHI). Per Jake Bulim's request, I successfully gathered and compiled information that would help solidify the company's needs in information security implementation and execution. The information provided in this report stems from documents written and published by the National Institute of Standards and Technology (NIST).

Attached to this document is an overview of each of the three NIST special publications (NIST SP 800-12 Rev. 1, NIST SP 800-100, and NIST SP 800-35) that were used to create the provided summaries. These documents are held in the highest regard as a starting point for both beginner and high-level frameworks that organizations build upon. It is my hope that these documents will provide the insight that was requested to better understand the needs and requirements of DHHI.

If the information I provided meets the set requirements, I would love to schedule a meeting for us to discuss next steps. Please do not hesitate to let me know if you have any further questions, comments, or concerns pertaining to any of the information in this report.

Sincerely,

Ethan Byrd

Cybersecurity Compliance Consultant

Ebyrd13@students.kennesaw.edu

678-630-9716 (Ext. 216)

Foundational Documents

The first publication, NIST SP 800-12 Revision 1, "An Introduction to Information Security," which operates as a high-level document meant to introduce several information security topics including roles, responsibilities, threats, vulnerabilities, and frameworks for the organization. Each chapter introduces the topics it will be covering and explains their importance to the organization's information security. Along with a foundational baseline, each chapter provides references to NIST documents that supplement further research of the respective subject matters. Along with foundational information from each chapter, the document provides eight major elements at the center of information security: its need to support the organizational mission; it is a crucial aspect of managerial success; it's implemented to help meet the risk tolerance and acceptance; each member of the organization has well defined roles; all department members must take their information security knowledge and apply it to all aspect of life; implementation will require a well-built foundation and blueprint; the organization must be monitored and assessed on a regular basis; and security is held within the confines of the culture that the organization has. These elements and baseline focused chapters will help this organization build a foundational understanding of information security while allowing for a customized approach to adapt the framework provided by NIST SP 800-12.

The successive publication, NIST SP 800-100, "Information Security Handbook: A Guide for Managers," provides a robust and comprehensive approach for Chief Information Security Officers [CISOs], agency heads, and security managers in helping to understand the requirements and implementation of information security management. It delves into topics such as the roles and responsibilities of key stakeholders and other related positions to ensure the

organization's information security approach aligns and conforms to business objectives and applicable laws. These positions play a continuous role in the assessment and monitoring of information security in the workplace such as awareness and training, security and contingency planning, risk management, and system development lifecycle. To provide meaningful security to the organization, managers must have a deep understanding, not just of what to do, but how to do it, and ensure stability. Without a solid managerial foundation there will not be a strong focus on security at any level of the organization.

The final reference document that will be notable is NIST SP 800-35, "Guide to Information Technology Security Services," which serves as a comprehensive guide to provide organizations with the knowledge on the implementation, selection, and management of security IT services while keeping a neutral stance by not prescribing or recommending any specific services, tools, or providers. NIST 800-35 keeps this neutral stance to allow companies the flexibility to build upon the recommendations and criteria set by the document. The document establishes early on the three IT security categories: Managerial, Operational, and Technical. These three categories outline different points of view the organization needs to have when implementing, assessing, or discontinuing assets and how it may affect other aspects of the organization. After the need for a new service is recognized, the guide provides a six-step IT security services lifecycle: initiation, assessment, solution, implementation, operations and closeout phase. These lifecycle phases allow decision makers such as CISOs, agency heads, and security managers to successfully implement these services and tools into their organization to best fit their needs.

References

Bowen, P., Hash, J., & Wilson, M. (2006). *Information security handbook: A guide for managers* (NIST Special Publication 800-100). National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.800-100

Grance, T., Hash, J., Stevens, M., O'Neal, K., & Bartol, N. (2003). *Guide to information technology security services* (NIST SP 800-35; 0 ed., p. NIST SP 800-35). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-35

Nieles, M., Dempsey, K., & Pillitteri, V. Y. (2017)**.** *An introduction to information security* (NIST SP 800-12r1; p. NIST SP 800-12r1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-12r1

DIAMOND HANDS HOLDING INC.

TO: Evan B., Michael P., Chase J., Dave F., William J., Issac W., Steve S.,

FROM: Ethan Byrd, Cybersecurity Compliance Consultant

SUBJECT: Applying Up-to-Date Information Security Strategies Using NIST

DATE: October 20, 2025

Dear Information Security team,

My name is Ethan Byrd, the Cybersecurity Compliance Consultant for Diamond Hands Holding Inc (DHHI). With DHHI's new announcement that we will be moving to a larger facility, I was tasked to successfully gather and assemble information that would provide value to the companies' needs in information security implementation and execution during the company's move. The information provided in this report stems from documents written and published by the National Institute of Standards and Technology (NIST). These documents are held in the highest regard as a starting point for both beginner and high-level frameworks that organizations build upon. It is my hope that these documents will provide the insight that was requested to better understand the needs and requirements of DHHI.

Attached to this message is an extensive report of the company's current directive and plans, along with the current goals set in place for the information security team. The report pulls examples from the publications I found: NIST SP 800-12 Rev. 1, NIST SP 800-100, and NIST SP 800-35. These publications will serve to help outline the company's goals for the information security team to implement them and build upon the set framework.

If the provided formal report is up to standard, I would love to find a time for us to meet and discuss next steps for the information security team. With the help of the information security team and these documents, DHHI will be able to make a smooth and safe transition to their new location.

Sincerely,

Ethan Byrd

Cybersecurity Compliance Consultant

Ebyrd13@students.kennesaw.edu

678-630-9716 (Ext. 216)

Applying Up-to-Date Information Security Strategies Using NIST

REPORT OF FINDINGS

Ethan Byrd

LAST REVISED OCTOBER 2025

EXECUTIVE SUMMARY

Diamond Hands Holding Inc. (DHHI) has launched a new growth initiative that includes relocating to a new facility, expanding the current workforce of the company, and regionalizing its service base through the acquisition of companies who own data and assembly centers, along with expanding the current workforce of the company. The company has found it imperative that all digital assets are properly protected and maintained in this transitional period. When researching relevant ways for these goals to be met, the documents that stood out the most were in the National Institute of Standards and Technology (NIST) database. The findings showed an overall weakness in our foundation and a need to update our standards with modern tools and services. Based on these findings, I have listed the NIST documents as a high priority reference. Using these documents will substantially increase the knowledge of managers and team members. The formal analysis will go into more detail on these ideas and why they should be used.

INTRODUCTION

Diamond Hands Holding Inc. is an Atlanta-based company that specializes in Governance Risk and Compliance and Information Security consulting services. DHHI is currently looking to expand to a new facility due to recent growth within the company. With this goal in mind, the company wants to ensure that the migration process goes as smoothly as possible, and all possible issues are to be resolved. The company's recent performance and revenue generation, combined with the upcoming move, promise success in receiving their capital funding investment request. Due to both initiatives, the company has been tasked with performing internal testing to ensure management and staff are prepared. We hope that these internal tests not only point out the flaws in the foundation but strengthen our risk stance and ensure its alignment with our company mission.

ANALYSIS

Nieles et al. in NIST SP 800-12 revision 1, provides a high-level baseline, teaching us to ensure that information security is at the center of the organization. This is outlined in the eight elements of information security, such as "Information Security supports the mission of the organization." And "Information Security is assessed and monitored regularly." (Neiles et al., 2017, p7). When implementing new tools and guidelines, if the DHHI Information security team can assure these eight elements, then it can be assured that we are protecting our digital assets. With the movement of the organization, it will fall upon management to ensure that these elements are enforced within their team. This is outlined in concept 6 which states that "Information Security roles are made explicit." (Neiles et al., 2017, p7). If management can ensure that roles are well-defined, then each member of the team will understand their task. With the team now in place, understanding things such as the organization's threats and vulnerabilities, risk tolerance, and

risk appetite will allow the information security team to implement the most protective and cost-effective measures. One of the risks outlined in the DHHI case study is the constant need and unexpected shift in technology and the availability of services. Keeping this risk in mind will prove to be useful when establishing a secure foundation.

Not only is strengthening the internal aspects of the organization crucial but so is understanding the importance of the security IT tools and services that are at the company's disposal. My recommendation for this area of expertise is NIST SP 800-35, written by Grance et al. This document is meant to help organizations evaluate the full impact that a service or tool will have on their organization. An organization that fails to take proper time selecting a service could risk financial loss and eroded (or diminished or damaged) trust with end users. NIST SP 800-35 provides organizations with a six-step IT security lifecycle for organizations, and the steps are as follows: initiation, assessment, solution, implementation, operations, and closeout. Within these six steps, there are no specific recommendations for the organization to use, allowing the organization the flexibility to update their security services and align with NIST guidelines as best as we can.

Outside of external services, there are also internal services that DHHI managers can provide to their employees to ensure security. I highly suggest using NIST SP 800-100 by Bowen et al., which helps outline the roles for managers and how they can provide the right tools and practices for their employees. By outlining the continuous role that you will all be playing for the organization, the information security team and all employees will have a stronger risk stance. Strengthening the organization can come in the form of educating and training your employees on how to safeguard their data and how to identify a threat such as a phishing scam. We can test vulnerabilities and discover organization vulnerabilities by using external services that match recommendations from NIST SP 800-35. If employees are aware of what to look for and what to avoid, the previously mentioned financial and trust damage can be avoided.

CONCLUSION

Based on the findings and recommendations in the analysis, there are steps that both base employees and management can make to improve information security at DHHI. Not only will these documents help implement new services, training, and security measures, but they also help provide guidelines for future upgrades and iterations of the Information Security framework at DHHI. If you find that the three provided documents are not enough or do not pertain to the needs of the organization, each of the documents provides references to other NIST document such as NIST SP 800-35 providing information on NIST SP 800-42 (Guideline on Network Security Testing). Overall, I know that the organization will gain great insight into information security and ensure a smooth transition during this time of change and movement.

References

Bowen, P., Hash, J., & Wilson, M. (2006). *Information security handbook: A guide for managers* (NIST Special Publication 800-100). National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.800-100

Grance, T., Hash, J., Stevens, M., O'Neal, K., & Bartol, N. (2003). *Guide to information technology security services* (NIST SP 800-35; 0 ed., p. NIST SP 800-35). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-35

Nieles, M., Dempsey, K., & Pillitteri, V. Y. (2017)**.** *An introduction to information security* (NIST SP 800-12r1; p. NIST SP 800-12r1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-12r1