## References

Bowen, P., Hash, J., & Wilson, M. (2006, October). NIST SP 800-100 Information security handbook: A guide for managers. Retrieved October 9, 2021, from <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf>

Hu, V. C., Iorga, M., Bao, W., Li, A., Li, Q., & Gouglidis, A. (2020). NIST SP 800-210 General Access Control Guidance for Cloud Systems. <https://doi.org/10.6028/nist.sp.800-210>

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006, August). NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response. Retrieved October 9, 2021, from <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-86.pdf>

NIST.gov. (2020, September). NIST SP 800-53 AU-6 AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING. Retrieved October 9, 2021, from <https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/control?version=5.1&amp;number=AU-6>

NIST.gov. (2021, September 30). Cybersecurity framework. CyberSecurity framework. Retrieved October 9, 2021, from <https://www.nist.gov/cyberframework>

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020, August 11). NIST SP 800-207 Zero trust architecture. Retrieved October 9, 2021, from <https://csrc.nist.gov/publications/detail/sp/800-207/final>

Ross, R., Pillitteri, V., Dempsey, K., Riddle, M., & Guissanie, G. (2021, January 28). NIST SP 800-171 Protecting controlled unclassified information in nonfederal systems and organizations. Retrieved October 9, 2021, from <https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final>

United States Computer Emergency Readiness Team, & US-CERT, The National Strategy to Secure Cyberspace (2003). <https://us-cert.cisa.gov/sites/default/files/publications/cyberspace_strategy.pdf>