

{Insert Date}

{System Owner Name}

{Insert Address – Please use your class level. E.g.: PhD Student in Cybersecurity at Marymount}

{System Owner Name},

The IT727A Security Office has completed the review of the {System Name} system’s security authorization package to ensure it meets the Cybersecurity Risk Management (IT727) class requirements. Based on the Federal Information Processing Standard (FIPS) security categorization of “{Low, Moderate or High}” and the provided Security Assessment, the IT727A Security Office has determined that the {System Name} system \_ meets \_ does not meet the information security requirements and is \_ granted \_ not granted an Authority to Operate (ATO).

If ATO has been granted, the security authorization of the information system will remain in effect for a length of time in alignment with Office of Management and Budget Circular A-130 as long as:

1. {System Owner Organization Name} satisfies the requirement of implementing continuous monitoring activities as documented in NIST 800-137’s continuous monitoring requirements and {System Name} Continuous Monitoring Plan;
2. {System Owner Organization Name} responds to all open low, moderate and high POA&M action items, agreed to in the Security Assessment Report (SAR) and as developed during the continuous monitoring activities; and
3. Significant changes or critical vulnerabilities are identified and managed in accordance with applicable Federal law, guidelines, and policies.

IT727A Security Office believes the security authorization package accurately documents the {System Name} system and clearly defines outstanding risk considerations.

**SIGNED:**

Microsoft Office Signature Line...

**Dr. Ibrahim Waziri Jr.**

{System Name} Authorizing Official (AO)

Chief Information Security Officer

Cybersecurity Risk Management (IT 727) Class

Marymount University, Arlington VA, 22203