CYBERSECURITY ANALYTICS
AND OPERATIONS

Degree Requirements
Master of Professional Studies (M.P.S.)
Requirements listed here are in addition to Graduate Council policies listed under GCAC-700 Professional Degree Policies (http://gradschool.psu.edu/graduate-education-policies/).

The M.P.S. program requires a minimum of 33 credits at the 400, 500, or 800 level, with at least 6 credits at the 500 level. A maximum of 9 transfer credits of high-quality graduate work may be applied toward the requirements of the degree, subject to restrictions outlined in GCAC-309 Transfer Credit (http://gradschool.psu.edu/graduate-education-policies/gcac/gcac-309-transfer-credit/). At least 18 credits must be courses at the 500 or 800 level, with at least 6 credits at the 500 level.

The 33 credits are distributed among the following requirements. A student first takes 18 credits of core courses. The student then takes 12 credits of electives. Lastly, the student must complete a culminating experience.

Elective Courses
The elective courses for the M.P.S. will be selected from a list maintained by the program office.

Electives
Select 9-12 elective credits from a list available from the program office.

Culminating Experience
The student may choose one of two culminating experiences for the degree: either the capstone project guided by the student's adviser and completed while enrolled in IST 594, or the capstone course IST 894.

Electives
Select 12 credits of electives from a list of approved electives available from the program office. The elective courses for the M.P.S. will be selected from a list maintained by the program office.

Culminating Experience
The student may choose one of two culminating experiences for the degree: either the capstone project guided by the student's adviser and completed while enrolled in IST 594, or the capstone course IST 894.

Electives
Select 9-12 elective credits from a list available from the program office.

Culminating Experience
Choose one of the following:

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>IST 594</td>
<td>Research Topics (Capstone Project)</td>
<td>3</td>
</tr>
<tr>
<td>IST 894</td>
<td>Capstone Experience (Capstone Course)</td>
<td>3</td>
</tr>
</tbody>
</table>

Total Credits
30

Master of Science (M.S.)
Requirements listed here are in addition to Graduate Council policies listed under GCAC-600 Research Degree Policies. (http://gradschool.psu.edu/graduate-education-policies/)

The M.S. in Cybersecurity Analytics and Operations requires a minimum of 30 credits at the 400, 500, 600, or 800 level, with at least 18 credits in the 500 or 600 series combined; 27 of the 30 credits must be earned at Penn State (refer to GCAC-309 Transfer Credit (https://gradschool.psu.edu/graduate-education-policies/gcac/gcac-309-transfer-credit/)). Students will be able to complete the proposed Master's program in one calendar year (including summer) or two academic years. All of the courses listed below are three credit hour courses, unless otherwise noted. Students pursuing the one-year format must complete the non-thesis track (IST 594). In addition, the one-year M.S. track must adhere to the following conditions:

- Students must take at least one credit of research (IST 594) for each of the three semesters (Fall, Spring, and Summer).
- A research adviser must be assigned to students in their first semester, as selection and discussion of the student's research topic must begin as soon as possible.
- Students who need more time to complete the final paper must be allowed to complete the paper, and have it reviewed and approved after the third semester (Summer) has ended. Students are not required to remain in residence while they complete the final paper. However, extensions granted to students in this program must comply with the Graduate Council policy on deferred grades (https://gradschool.psu.edu/graduate-education-policies/gcac/gcac-400/gcac-401-grading-system/).

These 30 credits are distributed among the following requirements:

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>IST 543</td>
<td>Foundations of Software Security</td>
<td>3</td>
</tr>
<tr>
<td>IST 554</td>
<td>Network Management and Security</td>
<td>3</td>
</tr>
<tr>
<td>IST 815</td>
<td>Foundations of Information Security and Assurance</td>
<td>3</td>
</tr>
<tr>
<td>IST 820</td>
<td>Cybersecurity Analytics</td>
<td>3</td>
</tr>
<tr>
<td>IST 825</td>
<td>Technologies for Web and E-Commerce Application Security</td>
<td>3</td>
</tr>
</tbody>
</table>

Electives
Select 9-12 elective credits from a list available from the program office.

Culminating Experience
Choose one of the following:

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>IST 594</td>
<td>Research Topics (Scholarly Paper)</td>
<td>3-6</td>
</tr>
<tr>
<td>IST 600</td>
<td>Thesis Research</td>
<td>6</td>
</tr>
</tbody>
</table>

Total Credits
30

Students can choose to complete a thesis or a scholarly paper as the culminating experience for the degree. Students who choose to complete a thesis must complete at least 6 credits in thesis research (IST 600 or IST 610). The thesis must be accepted by the advisers and/or committee members, the head of the graduate program, and the Graduate School, and the student must pass a thesis defense. Students in the non-thesis track must write a satisfactory scholarly paper while enrolled in IST 594 and complete at least 18 credits at the 500 level.